Research Journal of Applied Sciences 11 (10): 1039-1044, 2016
ISSN: 1815-932X

Hybrid Secure Conversation System

Bashar M. Nema
Department of Computer Science, College of Sciences, Mustansiriyah University, Baghdad, Iraq

Abstract: Communication and collaboration tools such as Instant messaging and Chat applications are broadly used applications in our today's life in all societies and for all fields. However the main problem that these applications suffer from is to ensure secure communication between the end-points which are involved in such communication in order to keep the privacy and secrecy of the transmitting information especially if these applications used in closed secret meeting system. In this study a proposed secure Instant messaging and Conference system will be built to support secure transport of the main triple media (text, audio, video) using a mixture of the most common security algorithms (RSA, AES, SHA512 and ECDiffie-Hellman) in the direction to achieve the basic three security goals (Confidentiality, Integrity and Authentication) for the different operations occurred in the proposed system.

Key words: Secure IM, secure chat, key exchange, CIA, ECDiffie-Hellman

INTRODUCTION

Instant Messaging systems (IM) and conversation chat applications are among the most growing and promising applications. IM is the private network communication between two users providing two basic elements; presence information and real-time messaging. The number of users for this application is growing year after year. The combination of presence awareness and real-time messaging offered by instant messaging and chat systems has proved to be the source of a killer application in the Internet which gathering hundreds of millions of users and although it was originally considered a teenager toy, the benefits of instant messaging have been realized by both academic and corporate organizations in the last few years (Salin, 2004).

Groups (Chat session) can be described as the public network communication between two or more users at the same time (Stalnacke, 2003).

But when coming to the design of IM and conferencing system, there is always at least one question concerning the security that must be answered before designing a system; how secure the system should be? The answer to this question is unfortunately very hard to answer because the security is a huge field that involved a lot of concepts that each related to one another. However the general goal when designing such systems is to create a system that is secure enough according to the total worth of the information used in the system in order to gain and keep the trust of the users (Li, 2005).

Transport protocols: However, as the Internet grows, its usage model and requirements are evolving. The limitation of current transport protocols to support both speed and reliability at the same time, push many companies and programmers to find solutions to this problem such as RTP (Real Time Protocol), this is especially effective in VoIP applications in order to send and receive voice traffic in most effective and reliable manner with minimum delay and distortion of the transmitting packets. In the end communications tools requirements will not stop at certain level.

As the development of computers moves in general towards speed, miniaturization and portability, communications development moves towards connectivity, interactivity and multimedia. When computers and communications are combined together we moved towards convergence, portability, personalization and cloud computing with all its associated communication, security and performance issues that related with them (William and Sawyar, 2005).

Quality of service: Quality of service is used to measure the degree of system performance according to the basic requirements that must be provided by the system. It is directly affects the ability of the system to meet the Service Level Agreement (SLA) that should be provided by the system. The cost-effective delivery of triple-play services (voice, data and video) is made possible in large part by next-generation, standards-based, distributed network architectures that use packet transport mechanisms. These new networks must deliver specific Class of Service (CoS) support for all three service types. In addition, each of these service types requires its own application-specific Quality of Service (QoS) needs (Williams, 2005).

Conversation system security: When using Instant Messaging (IM) and conferencing tools, many users and clients get feeling that their channels of communications are kept secure and that message sent can only be viewed by the intended recipient's. This can have devastating consequences in a system that does not use a sufficient level of security (Ivan, 2010). Some security concepts that will be used in the implementation of the secure conversation system and instant messaging system can be summarized as follow (Subramaniam and Subbaraya, 2015; Ne'ma and Ali, 2009):

- Asymmetric key cryptography
- Symmetric key cryptography
- Hash algorithms
- Key exchange agreement
- Elliptic curve cryptography

MATERIALS AND METHODS

Design of the proposed secure conversation system: The proposed system includes four public chat rooms in which the members (clients) can join any room and share secure (text, audio and video) conversations with other members. The text conversation is open such that the members can use it freely; however voice and video is limited to only six members at the same time for each room. Clients also have the ability to invite any member from any room to his private list and start secure (text, audio and video) private conversation with him. The proposed system consists of two main components:

- The server provide services and handle the management operations such as manage (room, requests, data base and security) and other operations
- The client request the services from the server and share in the public and private conversations

Proposed cryptographic scheme specification: This section will describe how the security base is applied upon the proposed conversation system. The main goal of this security base is to prevent an adversary to read or intercept the conversation messages so as to retain the privacy among the users of the application. The basic goals by the following points:

- Ensure secure public conversation between the room members
- Provide secure private conversation between any two peers without the intervening of the server
- Secure register/login
- Protect a user from inserting weak username and password
- Secure exchange of room keys and session keys
- Secure session key exchanging for P2P traffic
- Other complementary features that could be used under the term security. These are:
  - Prevented list word to prevent specific words to be displayed for the user
  - Switch on/off to allow the user to lock the program securely without the need to close the session
  - Chat monitor to determine the time used for chatting before closing the program automatically

The proposed security base uses a mixture of (AES, RSA, SHA512 and ECCDiffie-Hellman) algorithms. Table 1 shows the main functionality and the default parameters by these algorithms. These algorithms are applied to the system through many operations occurred in the system. These operations will be illustrated as request/response scheme (Table 2):

Start Secure Communication request (SSC):

- Key symbols
  - SPu: Server public key for RSA algorithm,
  - SPr: Server private key for RSA algorithm.
  - S1: Server public key for ECDiffieHellman,
  - D: SHA-512 digest , Sig: Signature.
- Request pseudo code:

Register/Login request:

- Key symbols:
  - S2: Client public key for ECDiffieHellman)
  - M: Message Authentication Code (MAC

Table 1: Default parameters for the used cryptographic algorithms

Algorithm	AES	RSA	SHA512	ECCDH
Main functionality	Confidentiality	Confidentiality authentication	Integrity authentication	Key exchange
Default parameters	Key size: 256 bits Op. mode: CBC	Modulo size: 1024 bits	Digest size: 512 bits	Key generation size: 256 bits

Table 2: Communicate with CSS

Events	Description
Flow of events	Ali chooses to register to CSS. Ali fills the form by inserting Ali username and password and encrypts the information using Client register step security policy. Ali sends the encrypted information to server. CSS server decrypts the information according to Server register step security policy and adds Ali account to CSS Data base CSS send accept signal to Ali Ali use the new username and password to login to CSS successfully

Scenario name: Success Register; Participating Initiated by Ali: Actors Communicate with CSS

- SHc-s: Shared AES temporary symmetric key between the client and server
- Uc: client username
- Pc: client password
- SDB: Server data base

- Request pseudo code:
  - S1: Client public key for ECCDH algorithm,
  - S2: Server public key for ECCDH algorithm.
  - SH2c-s: Second shared AES temporary symmetric key between client/server
  - Rk: AES Room key
  - SSk: AES server session key
  - M: Message authentication code

Join room request:

- Key symbols:
  - SPu: server public key for RSA algorithm
  - SPr: server private key for RSA algorithm

Share public conversation request:

- Key symbols:
  - Rk: AES room key
  - SSk: AES sever session key
  - Sref: Reference address to cam/voice
- Request pseudo code:

Invite member request:

- Request Pseudo code:

Share private conversation request:

- Key symbols:
  - K1: Sender AES key
  - K2: Receiver AES key
- Request pseudo code

System implementation: Using Microsoft Visual Studio 2010, for the greatest features it provides to develop complex systems perfectly; the proposed system was implemented using C# language by exploiting the rich functionality provided by the system in addition to other external API interface to capture and play video and voice media. Generally System interfaces are designed to be easily used by the users. Figure 1 and 2 shows the main interface in both server and client.

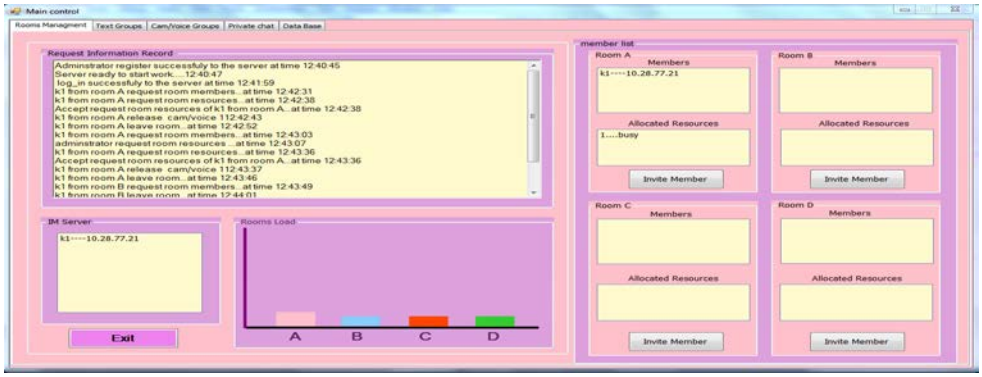

Fig. 1: Server room management interface

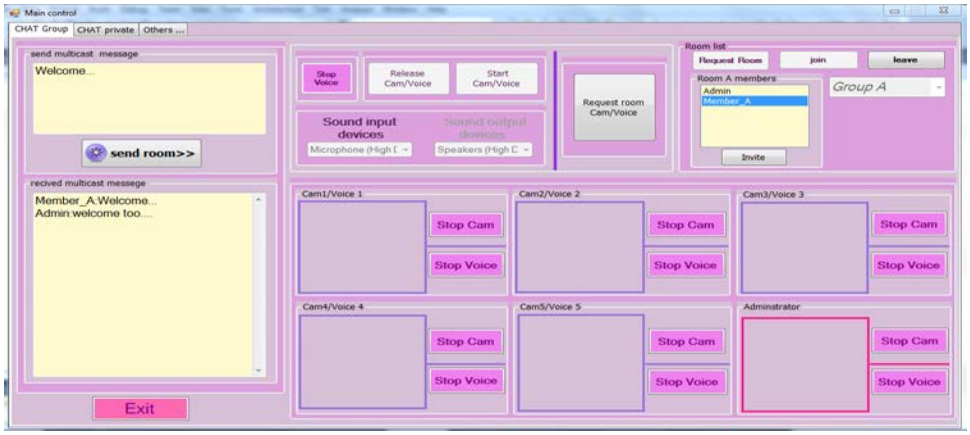

Fig. 2: Client room management

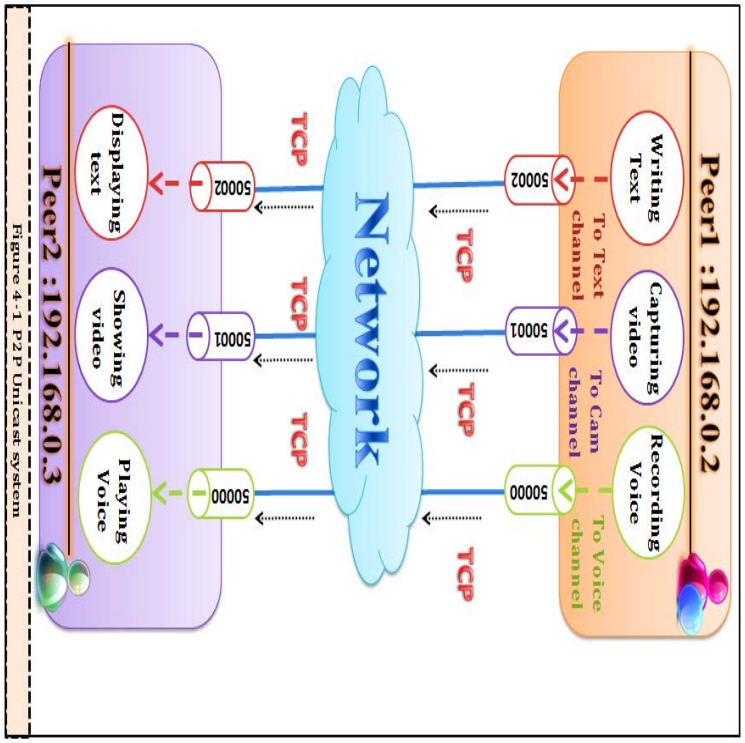

Fig. 3: Proposed system TCP and Port

Figure 3 show the general view of the proposed system and the network ports that classified and used depends on the type of conversation (Text, Voice, or Video).

RESULTS AND DISCUSSION

Security traffic analyses: Security cryptographic operations, all happened behind the scene, there is no visible distinct between the system before and after applying cryptographic operations on the data. For this reason some tools is needed that enable to analyze the traffic before and after applying these operations. For text analysis Wireshark is used. Wireshark is the most popular software that can be used to analyze packet traffic across the network. Figure 4a and b shows the same captured message (Welcome Room member…) before and after applying the cryptographic scheme. It is obvious that the captured message by wireshark before encryption is clearly readable. However, the same message became unreadable and could not be understood after encryption. This indicates that the attacker could not break the confidentiality of the transmitting messages since the key is unknown for him.

For video encryption video encryption tester is used to display the video before and after decrypting the

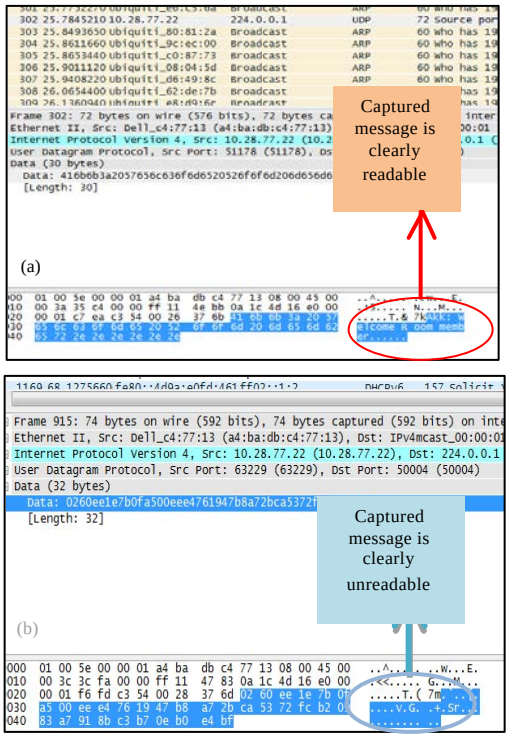

Fig. 4: Captured message before and after encryption using Wireshark

Fig. 5: Captured video before and after encryption

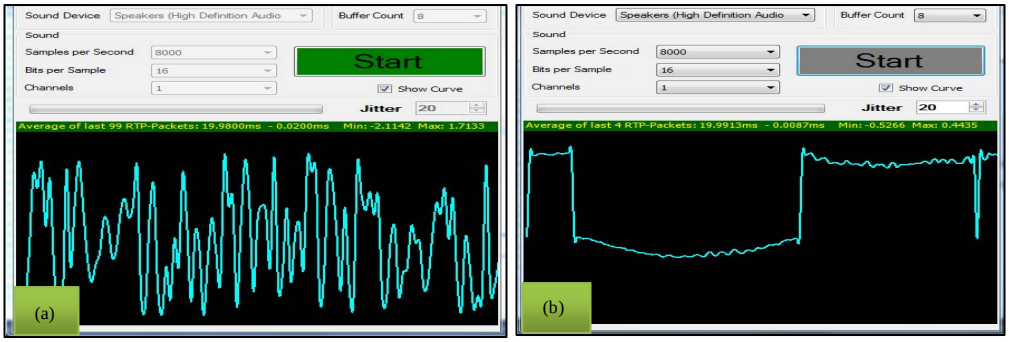

Fig. 6: Captured voice signal before and after encryption

traffic. In this case the visual information could be used to easily compare the crabbed video before and after applying the cryptographic scheme. Figure 5 shows the result of a captured frame before and after decryption.

It is obvious that the encryption frame is totally unfeasible and could not recognize anything that appeared in the same frame after decryption. To evaluate the encryption performance of voice traffic a frequency drawer is used. The result of voice encryption is shown in Fig. 6a and b. As it could be seen that the encrypted voice signal shown in Fig. 6b is totally distinct from the original voice signal and it is randomly distributed like a noise signal while the signal distribution in Fig. 6a is completely flat and uniform at two extreme ends. This shows the effectiveness and suitability of the proposed scheme for voice data encryption.

CONCLUSION

Through building the proposed secure conversation system, the following points could be concluded:

- There is no system that is fully secure. This is because the huge concepts covered by the term "Security". This requires the work of an expert team, not just one or two simple programmers
- Reinforcing by a trusted security computing base should not affect the average performance of the whole system
- The developer should think carefully before designing a secure system about the general goals and the type of the users who will use that system in order to meet the predetermined requirements in efficient and reliable manner
- Using the most powerful security tools is not enough unless the developer know how to use them effectively. This has great effect on the whole security performance of the system

REFERENCES

Ivan, K., 2010. Novel approaches to P2P traffic optimization. M.Sc Thesis, Department of Computers and Informatics, Technical University of Kosice, Kosice, Slovakia.

Li, Y., 2005. Secure group communication protocol and implementation for Jet Meeting an application based on P2P. Master Thesis, Iowa State University, Ames, Iowa.

Ne'ma, B. and H. Ali, 2009. Multi purpose code generation using fingerprint images. Int. Arab J. Inf. Technol., 6: 418-423.

Salin, P., 2004. Mobile instant messaging systems-a comparative study and implementation. Master Thesis, Helsinki University of Technology, Espoo, Finland.

Stalnacke, F., 2003. Implementation of an instant messaging client using the OMA IMPS protocol. Master Thesis, Umea University, Umea, Sweden.

Subramaniam, U. and K. Subbaraya, 2015. A biometric based secure session key agreement using modified elliptic curve cryptography. Int. Arab J. Inf. Technol. (IAJIT.), 12: 155-162.

William, B.K. and S.C. Sawyar, 2005. Using Information Technology. 6th Edn., McGraw Hill Publishing Co., USA., pp: 3, 4, 147.

Williams, J., 2005. Troubleshooting IP video quality of service. White Paper, JDS Uniphase Corporation, Milpitas, CA., USA. http://www.viavisolutions.com/sites/default/files/technical-library-files/IPVIDEOQOS_WP_ACC_TM_AE.pdf.