Secure Messenger System Using Both Cryptographic And Steganographic Techniques in Webcam Frame

Associate Prof. Dr Ali Makki Sagheer
Mohammed Adeeb AbdulJabbar
Information System Department College of Computer-University of Anbar

Abstract

In this project we tried to maximize the level of security needed to send some messages among users. To do this, a number of programming tools have been used to support this project. The design of the system includes a four steps process, the first two occur at the sending station and the other two are at the receiving station. The processes are (Encryption, Hiding, Decryption and Revealing) sequentially. The project is designed to open one port between the connecting stations which the video port. The sender will write a message and when the send button is clicked the message will be encrypted and the frame captured at that moment will be the carrier file. The message then goes to a hiding process and then at receiving station the process backward.

1. Introduction

Information is one of a financial institution's most important assets. Protection of information assets is necessary to establish and maintain trust between the financial institution and its customers, maintain compliance with the law, and protect the reputation of the institution. Timely and reliable information is necessary to process transactions and support financial institution and customer decisions[1].

Information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintain

Information vital to its operations. On a broad scale, the financial institution industry has a primary role in protecting the nation's financial services infrastructure. The security of the industry's systems and information is essential to its safety and soundness and to the privacy of customer financial information[2].

A financial institution establishes and maintains truly effective information security when it continuously integrates processes, people, and technology to mitigate risk in accordance with risk assessment and acceptable risk tolerance levels. Financial institutions protect their information by instituting a security process that identifies risks, forms a strategy to manage the risks, implements the strategy, tests the implementation, and monitors the environment to control the risks[3].

The messenger is one of today's biggest important applications on the Internet. It is a means of communication among people through different types of media (i.e. Text chatting, Audio conference, video, and file sharing … etc). This technique has made a great revolution in network programming and though become a target for hackers and intruders. The messenger opens a real-time transmission line (live) among a group of people (usually two), so the major concern is keeping the high speed of transmission while having a very high level of privacy. This means that a messenger builder must use an efficient algorithm for encryption and decryption that provides a good security while using the minimum time required to work. The rapid change in transmission technologies and transmission medium and with new techniques being provided the job of speeding up transmission becomes easier and easier, the challenge today is to preserve security[4].

2. Related Work

Many of the systems being developed in this area relays on providing a single security service (i.e. either Encryption or Steganography). Using the two fields together brings a great advantage to a system and there are some systems that uses both techniques. Studies about those fields are not present, they go way back to the beginning of computers. For atimeline that includes studies of computer and network security, (see Table 1).

In 2008 Bin proposed A global frame of secure instant messaging system based on Microsoft MSN to solve the security problems that exist in instant messaging. The results of the performance test of the add-in and key management module show that, in the precondition of being compatible to MSN, the system could solve the secure problems between instant messaging users such as key management, identity authentication, message encryption and authentication etc[5].

Rui in May 2010 designed and implemented a system based on the deep analysis of IM texts, files and audio protocol characteristics, an instant messenger monitoring. By means of capture techniques of network data packets, protocol characteristic identification techniques based on regular expression, and storage strategy for transfer files, Rui presented a monitoring system can monitor texts, transfer files and audio data of many instant messenger tools, such as MSN, ICQ and QQ. At the same time, He was able to resolve the problem raised by version upgrade of IM software by means of adding new rules based on protocol characteristics[6].

In July 2006 , Raymond B. Jennings III, Erich M. Nahum, David P. Olshefski and Debanjan Saha presented a taxonomy of different feature and functions supported by most common systems, namely, AOL Instant Messenger (AIM), Yahoo Messenger (YMSG), and MSN Messenger (MSN). They have also examined the system architectures and protocols that power these systems[7].

Hiroaki in 2004 studied a security enhancement of instant messaging service. After the requirements and the assumptions are addressed, a modified Diffie-Hellman protocol suitable to instant messaging is presented. The main feature of the protocol that Hiroaki proposed is to prevent malicious administrator from intercepting plain message and applying data mining techniques to obtain privacy of end users. From the viewpoint of communication and computational costs, the proposed protocol are evaluated and the comparison of some existing protocols isgiven. In addition, a trial implementation of secure instant messaging system is demonstrated[8].

In 2009, Qiushi Yang and Yvo Desmedt observed that the way how feedbacks were used in previous work does not guarantee perfect privacy to the transmitted message, when the adversary performs a Guessing Attack. They described a new Guessing Attack to some existing protocols and propose a scheme defending against a general adversary structure. In addition, they also show how to achieve almost perfectly secure message transmission with feedbacks when perfect reliability or perfect privacy is not strictly required[9].

Documents	Date
Maurice Wilkes discusses password security in Time-Sharing Computer Systems.	1968
Schell, Downey, and Popek examine the need for additional security in military systems in "Preliminary Notes on the Design of Secure Military Computer Systems."	1973
The Federal Information Processing Standards (FIPS) examines Digital Encryption Standard (DES) in the Federal Register.	1975
Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," discussing the Protection Analysis project created by ARPA to understand better the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software.	1978
Morris and Thompson author "Password Security: A Case History," published in the Communications of the Association for Computing Machinery (ACM). The paper examines the history of a design for a password security scheme on a remotely accessed, time-sharing system.	1979
Dennis Ritchie publishes "On the Security of UNIX" and "Protection of Data File Contents," discussing secure user IDs and secure group IDs, and the problems inherent in the system.	1979
Grampp and Morris write "UNIX Operating System Security." In this report, the authors examine four "important handles to computer security": physical control of premises and computer facilities, management commitment to security objectives, education of employees, and administrative procedures aimed at increased security.	1984
Reeds and Weinberger publish "File Security and the UNIX System Crypt Command." Their premise was: "No technique can be secure against wiretapping or its equivalent on the computer. Therefore no technique can be secure against the systems administrator or other privileged users...the naive user has no chance."	1984

Table (1.1) timeline of studies of computer and network security

3. The Proposed System

The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit. The academic disciplines of computer security, information security and information assurance emerged along with numerous professional organizations - all sharing the common goals of ensuring the security and reliability of information systems.

In this messenger the encryption technique used is (RC4). The system is divided into a number of processes:

1- Select a device to start (camera).

2- Enter some text.

3- Encrypt that text.

4- Choose the frame arrived at that moment.

5- Hide the ciphertext in the frame.

6- Send that frame.

These steps are going for encryption and sending process and the same process is performed for receiving and decryption but in reverse order (i.e. Receive frame, Reveal message, Decrypt, Show message).

The whole system module is shown in Figure (1) below:

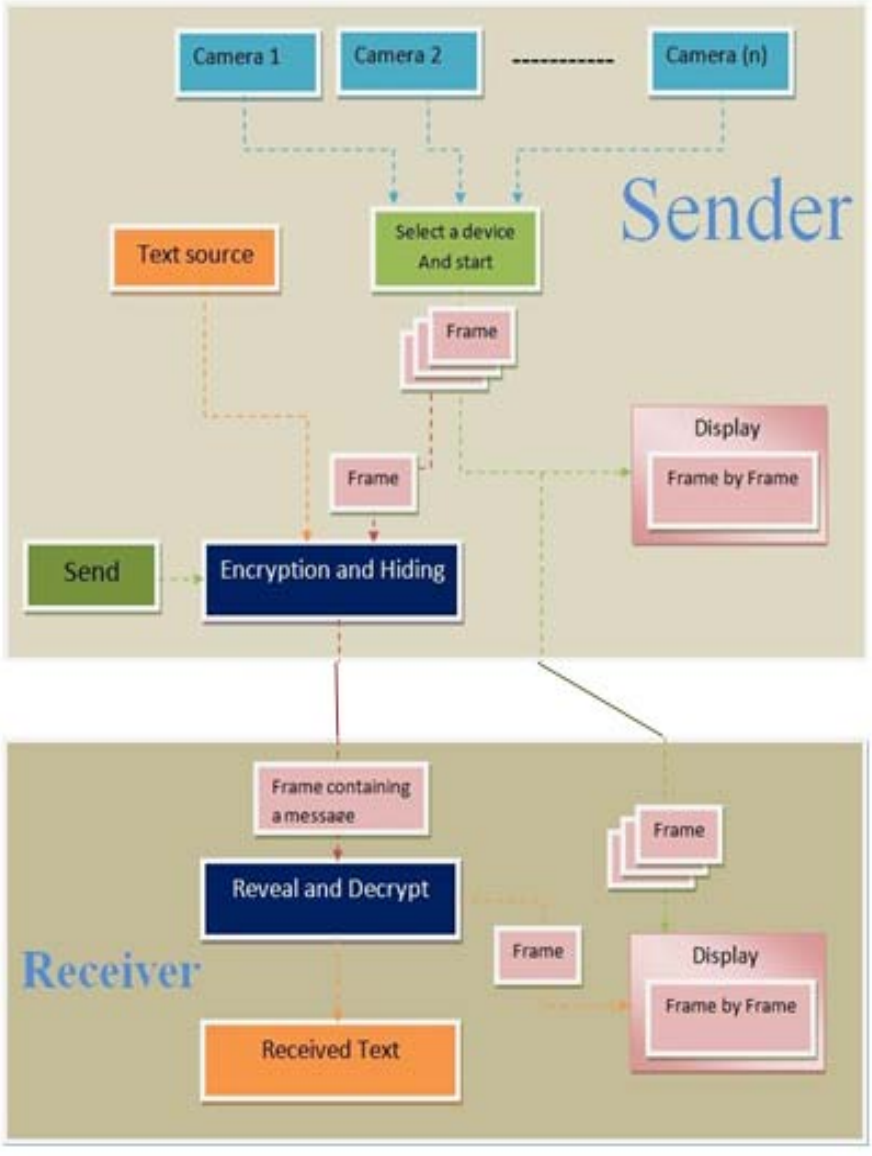

Figure (1) The Whole System Module

4. Conclusion

1- The messenger has three levels of security:

- ☐ Fooling the hacker that the data being transmitted is only images while it has some message in it.
- ☐ If the technique is known then it will be very hard to process (24) frames per second to get some cipher text.
- ☐ And if the ciphertext text is known, the hacker (intruder) will have to decrypt that piece of text to get some plain text.

2- There might be some risks of losing some data during transmission due to noise in transmission channel or limited transmission speed…etc.

3- This technique is very easy theoretically but it has so many difficulties like applying a suitable algorithm for encryption so that less time will be required to prepare some cipher text, therefore we used RC4 for its encryption speed.

4- In order for this messenger to work a computer must meet some requirements so that no time will be lost. This means that this project is only useful for close-up communication for reasonable computers; else some requirements must be met.

5. Future Work

1- To achieve a good performance for such kinds of messenger, a full system test must be made on different types of transmission mediums (wireless, wired).

2- A new encryption algorithm may be created or an existing one modified to have a whole new (unbreakable) system.

3- Also a good algorithm of hiding information is required to achieve high speed of transmission. Also a camera with a good resolution may be chosen to have more accurate hiding and retrieval.

References

1- Sung Woo Tak, Yugyung Lee, Eun Kyo Park, and Jerry Stach, " Design and Evaluation of Adaptive Secure Protocol for E- Commerce ", 2001, IEEE

2- Klensin, "Simple Mail Transfer Protocol", 2001, IETF RFC 2821

3- C. E. Landwegr, C. L. Heitmeyer, and J. D. McLean, "A security model for military message systems: Retrospective", 2001, Naval Research Laboratory, Wasgington, DC

4- T. R. Surmacz, "Reliability of e-mail delivery in the era of spam", 2007, International Conference on Dependability of Computer Systems, DepCoS-RELCOMEX'07, 198 – 204

5- Bin Zhang, " Design and Implementation of Secure Instant Messaging System Based on MSN ", 2008, Computer Science and Computational Technology, ISCSCT '08

6- Lu Rui, " Design and implementation of instant messenger security monitoring system based on protocol analysis ", 2010, Control and Decision Conference (CCDC), Chinese

7- Raymond B. Jennings III, Erich M. Nahum, David P. Olshefski and Debanjan Saha, " A Study of Internet Instant Messaging and Chat Protocols ", 2006, IEEE

8- Kikuchi Hiroaki, " Secure instant messaging protocol preserving confidentiality against administrator ", 2004, 18th International Conference on Advanced Information Networking and Applications, AINA

9- Qiushi Yang and Yvo Desmedt, " Cryptanalysis of Secure Message Transmission Protocols with Feedback ", 2009, RCIS, AIST, Japan