Chapter 1

`INTRODUCTION

Background of the Study

Data exchange or data communication is a key process of providing accurate and timely information to senior leaders, top management, and decision makers. It involves the use of email, instant messaging, video conference, chat, online forums, and other applications that transmit data from sender to receiver. Many organizations and modern companies prefer to use instant messaging rather than email for simpler and more user-friendly collaboration among staff and management. It also exchanges data almost at an instant, allowing two-way communication in near real-time.

Instant messaging applications like Facebook messenger, SKYPE, and Yahoo Messenger provide easy, fast, and cost-effective means of text, voice, and video communication. It has become the most preferred application to communicate with peers, families, and among professionals from various industries and sectors. Businesses are now beginning to embrace IM for their office communication. Although it is less formal than a face to face meeting, it can bridge the gap of needing to collaborate and communicate with each other. Private companies, schools, organizations, and government agencies use IM to support or provide redundancy with their other existing mode of communication.

The military recognizes the necessity to develop or acquire a secure, reliable, and near real-time data communication tool for effective exchange of information and to provide the high-command a means to collate information needed for decision-making. In

today's network-centric operation, Instant Messaging (IM) is an essential information communication tool for rapid delivery of messages and reports, and for situational awareness.

The US military has long been using IM for its military operations. In fact, Cummings (2004, p. 654) stated that "it was the primary means of communication between navy ships during Operation Iraqi Freedom in 2003". The Philippine Navy (PN), a branch of service in the Armed Forces of the Philippines (AFP), sought to acquire similar tool but is constrained with limited resources and lack of communication infrastructure to securely extend its network to mobile units thereby utilizing the un-secure Internet for its data communication.

The PN, with its prevailing need for a secure data communication like an instant messaging, started to adopt several free and open-source IM but unsatisfied with the minimal encryption it provides. Text messages can be intercepted, decoded, and read in clear text as it travels across the network from sender to receiver. The pervasiveness of these applications makes it vulnerable from various attacks especially sniffing and hijacking. Some vendors, however, promise end-to-end or asynchronous encryption with their expensive commercial IM. They may either use open-standard advanced encryption protocols or they are using closed and proprietary protocols. The benefit it provides may surpass that of the free versions, however, the vendor obscures any vulnerabilities of this application from the end-users and it will not be long until a sophisticated hacker can crack its encryption protocol through a purchase of similar application.

Among the popular IMs available online are unencrypted by default such as Facebook Messenger, Pidgin, Google Allo, and Viber. IMs are designed with usability

rather than security in mind. Almost all freeware IM software does not have encryption capabilities.

Few news articles can be found as an evidence of this vulnerability, many IM vendors bargain this flaw as leverage for the users to purchase the licensed version. Eavesdropping and sniffing IM conversation is common to most hackers and cybersecurity professionals especially if they are within the Local Area Network (LAN).

Data security is of utmost importance in any organization whether private or government sector. The effect of confidential messages being sniffed, leaked, or compromised can be devastating to any individuals, businesses or institutions such as the Armed Forces. Quality of software should be measured not just by the functionality and performance but also the security it guarantees. It has to assure the confidentiality, integrity, authenticity, and availability of the data it processes. Thus, adoption of an encryption mechanism is imperative to secure the data at-rest or in-transit.

The growing importance of security for an IM or for any type of application cannot be overemphasized. All communication application (i.e Instant Messenger) must be integrated with an encryption algorithm that is proven unbreakable and resistant to any mathematical cracking techniques. With an encryption component present in an IM, users are assured of an optimum level of security the software provides.

Data hiding or Steganography has been used to hide secret messages into an image. While it is commonly used as a standalone application, it has never been implemented into an IM. Integrating both encryption and steganography is a research worth exploring.

Secure IM is sought to benefit primarily the PN, and the AFP. Other sectors such as business offices, government agencies, schools, industries, banks, and other institutions can also adopt this software for office communication, report collection, and information dissemination.

Objectives of the Study

This study aims to develop an Instant Messaging desktop application called Cryptographic Instant Messaging (CIM) system.

Specifically, the study aims to:

1. Design CIM system with the following features and characteristics:
    a. Multi-layer encryption by combining Advance Encryption Standard (AES) algorithm and Hidden In Plain Sight (HIPS) image hiding technique;
    b. Secure One-to-one and room chat using AES algorithm;
    c. Secure File transmission using the combination of AES 256-bit encryption and HIPS;
    d. Secure login authentication through password encryption;
    e. Transmit recorded voice message;
    f. Self-delete or automatic deletion of secret message;
    g. Use of cipher key exchange methods:
        1) System Generated Key (SGK); and
        2) Manual Key Input (MKI).
    h. Encrypted username and password on the database
    i. The users decrypt the file at the time of their choosing.

2. Develop the desktop application using Visual C# .net, as designed
3. Test the functionality and security of the system across different Penetration Testing software.
4. Test the portability of the system across different multiple versions of MS Windows operating system.
5. Test the latency of data transmission when dual-layer encryption is applied.
6. Evaluate the quality of the software using ISO 25010 with criteria for Functional Suitability, Performance Efficiency, Usability, Reliability, Security, Maintainability, Portability, and Compatibility.

Scope and Limitations

The development of Cryptographic IM (CIM) system is inspired by the PN's desire to develop a data communication tool that provides secure data exchange and rapid delivery of reports and messages.

The system has the essential features of a typical IM such as one-to-one chat, room chat, and file transfer. It is designed and developed in modules or components and provides the platform that allows other library/API/modules to be integrated into.

The CIM integrates AES 256-bit algorithm and HIPS hiding algorithm by Engr. Mardonio M Agustin Jr. to provide multi-layered encryption. It has two (2) methods of key exchange: SGK and MKI – the former is the default setting whereby randomly generated keys are pushed on every IM Client every week while the latter allows user to type in the keys manually for a guaranteed privacy among peers.

It is developed using the client-server architecture whereby the server relays all messages among connected clients. It uses Microsoft Visual C# for coding. It runs on any computers with MS Windows operating system.