CHAPTER 6 EVALUATION AND CONCLUSION

6.1 Achievements

This Section mentioned about research's achievements from it started till the end. The achievements include theoretical knowledge, practical information, management view and other new technology.

6.1.1 Theoretical Knowledge on Network

In order to understand the concept of network, we have to understand Open Systems Interconnection (OSI) first. OSI is a standard description or "reference model" for how messages should be transmitted between any two points in a telecommunication network. The reference model defines seven layers of functions that take place at each end of a communication.

The main idea in OSI is that the process of communication between two end users in a telecommunication network can be divided into layers, with each layer adding its own set of special, related functions. Each communicating user is at a computer equipped with these seven layers of function. So, in a given message between users, there will be a flow of data through each layer at one end down through the layers in that computer and, at the other end, when the message arrives, another flow of data up through the layers in the receiving computer and ultimately to the end user.

6.1.2 Theoretical Knowledge on Network Security

Any network connection consists of three parts: the client, the server and the connection between the two. As a network connection has three parts, network security also has three parts.

- Client-side security. These are security measures that protect the user security of his / her computer. Technological solutions include safeguards to protect users against malicious activities. Client-side security can be guaranteed by

E-PAP system, as authentication is the most important of the security services because all other security services like access control, confidentiality, integrity and non-repudiation depend upon it.

- Server-side security. These are measures that protect the server and the machine it runs on from break-ins, site vandalism and denial of service attacks. Technological solutions run the gamut from firewall systems to operating system security measures. By using E-PAP System, it can provide authentication service that is the most important security service among other services.
- Connection security. These are measure to protect information from being disturbed by third parties. E-PAP System can protect information by providing authentication service.

6.1.3 Theoretical Knowledge on Windows Socket

The Windows Sockets Specification has been built upon the Berkeley Sockets programming model that is the de facto standard for TCP/IP networking. It is intended to provide a high degree of familiarity for programmers who are used to programming with sockets in UNIX and other environments, and to simplify the task of porting existing sockets-based source code. The Windows Sockets API is consistent with release 4.3 of the Berkeley Software Distribution (4.3BSD).

By defining header as below:

```
#ifndef WIN32
#include <winsock.h>
#endif
```

The header files provided above are compatible with following headers in BSD:

```
netdb.h
arpa/inet.h
sys/time.h
sys/socket.h
netinet/in.h
```

The file winsock.h contains all of the type and structure definitions, constants, macros, and function prototypes used by the Windows Sockets specification.

6.1.4 Practical Knowledge

Besides the theoretical knowledge, this research also improves technical experience. During the development of E-PAP System, the Microsoft Windows family operating system kernel, installation and its configuration files like `system.ini`, `win.ini` and Registry was reviewed. The actual Windows family operating system process is reviewed in order to identify hardware, network connection and the file located. The Windows API about how to disable some special key like `Escape`, `Ctrl + Alt + Del` and `Alt + Tab`, `Alt + F4` also is investigated.

6.2 Future Enhancement

6.2.1 Multithreaded Server

This version of E-PAP Server able to accept maximum five requests from E-PAP Client(s) simultaneously. However, the server is a single-threaded server and only able to process one request in a time. The future version of E-PAP Server will be a multithreaded and able to process every request for each connection in a time.

6.2.2 Internet Standard for E-PAP System

Currently, there are two schemes for HTTP's authentication framework: Basic Access Authentication and Digest Access Authentication [10]. Basic Access Authentication scheme in HTTP/1.0 in [20] has been implemented in most Web browsers like Netscape Navigator (all version), Internet Explorer (all version), Opera (all version) and supported by most of Web Server like Apache Web Server and IIS Web Server (all version). Digest Access Authentication scheme in HTTP/1.1 [21] that was proposed in June 1999 has been implemented in some Web Browsers like Internet Explorer version 5 and is supported by some of Web Servers like IIS Web

Server version 5. Algorithms like MD5 in Digest Access Authentication are carried out by Web browser (client part) without any external program or plug in.

To implement zero-knowledge proof strong authentication like E-PAP for Internet case, an external program or plug in must be called out as all these algorithms has not yet built in Web browser. Therefore, a new request for comment (RFC) that specifies an Internet standards track protocol for the Internet community about zero-knowledge proof strong authentication must be worked out. For more detail about the process of creating an Internet Standard, please refer to RFC 2026 [68].

6.3 Conclusion

Finally, the dissertation titled "Enhanced Password-Based Authentication Protocol" was successfully done. It covers every single scope that mentioned in scope of the dissertation.

In the process, invaluable insight was gained into the complexities and intricacies of programming by using Visual C++. Knowledge gained throughout the life cycle of project development, from the planning of the project, studies on the subject and technologies, setting up of servers, programming, to implementing the system proves to be a valuable experience. At the same time, theories and knowledge gained throughout the course of computer science studies were put into practice. This experience will definitely prove useful in future software development projects.

There are still many rooms for improvement in E-PAP System. The successful development of E-PAP System is the first step towards the future development of similar systems. It is hoped that E-PAP System can provide a foundation upon which more enhanced versions may be created.