CHAPTER 5 TESTING AND RESULTS

5.1 Purpose and Assumptions

5.1.1 Purpose

The purpose of the testing was to investigate the effectiveness of the E-PAP System. This will help the operating system from being attacked or threatened by hackers. The testing is to determine the strengths and limitations of the E-PAP System.

5.1.2 Assumptions

During the testing period, all the computers that carry out E-PAP server and E-PAP client are free of any keylogger application. Keylogger is an application that runs in the background and saves (almost) all keys the user press to a text file. A keylogger is a very convenient way to find out logon names, passwords and other information. This assumption is made because even if an authentication system is the best and most powerful in the world, it is useless because of the password is stored in a plain text file by a keylogger.

5.2 Participants and Venue

The E-PAP System was tested by 3 participants, all of them were voluntary students pursuing their Master in Computer Science at Faculty of Computer Science and Information Technology, University of Malaya (UM). The venue for testing is in the Master Lab, First Floor, FSKTM Building. All of the computers in this labs are Pentium II 233MHz, 32MB RAM with Microsoft Windows 95 platform. The computer used by the author acted as E-PAP Server, the author acted as the administrator who monitored the system and the computers used by participants acted as E-PAP Clients. The testing was scheduled to be conducted in one session each day from 15/5/2000 to 17/5/2000. As there was shortage of volunteers, each participant managed two E-PAP Clients.

5.3 *Procedures*

The first step in conducting the testing was to install an E-PAP Server on one computer and E-PAP Client on six computers. Six new users (test01, test02, test03, test04, test05 and test06) were generated by the administrator (Table 5-1). Both user logon names and their passwords with eight alphanumeric characters were randomly chosen by the system. Then, user logon names and their passwords were written down in a piece of paper and were given to the three participants (two users for each participants) confidentially. After that, all participants' computers were restarted. The E-PAP Server was started manually by administrator. All E-PAP Clients were started automatically after the original Client For Microsoft Network Logon (Figure 4-12) for Windows 95 appeared.

Table 5-1: IP address, host name and user.

	IP Address	**Host Name**	**Participant**
1.	10.100.1.150	aust11	Administrator
2.	10.100.1.151	aust12	test01
3.	10.100.1.152	aust13	test02
4.	10.100.1.153	aust14	test03
5.	10.100.1.154	aust15	test04
6.	10.100.1.155	aust16	test05
7.	10.100.1.156	aust17	test06

5.4 *Testing and Result*

The testing was carried out in 6 phases for each session from 15/5/2000 to 17/5/2000. To simplify the results, only the results of user test01 were showed unless mentioned.

5.4.1 Phase I: Generating a Credential

(Phase I was carried out by the administrator.)

Testing	Result
Typed `generate` in dos command prompt.	Administrator was prompted to provide a user logon name.
(Continued from above) Administrator provided a user logon name: `test01`.	A user list file `user.txt` was automatically built and registered `test01` as a new user, and created a credential files `test01.ver` with random password `Bo3jvmOj`.
Administrator provided user logon name: `test01` again.	A message "`test01 is already registered. Please choose other name.`" appeared.
Administrator provided other user logon name: `TEST01`.	A message "`TEST01 is already registered. Please choose other name.`" appeared, as the logon name is not case-sensitive (all logon names are stored in lower case in `user.txt` file).

5.4.2 Phase II: Starting E-PAP Server

(Phase II was carried out by the administrator.)

Testing	Result
Typed `server` in dos command prompt.	Administrator was prompted to provide a port number.
(Continue from above) Administrator provided a port number: `port#`.	A message "`Please provide port number between 49152 and 65535`" appeared as port number does not take alphabet.
(Continue from above) Administrator provided a port number: `51688`.	A message "`Welcome to E-PAP Server! host = aust11 Waiting to accept a connection ...`"

	appeared as E-PAP Server with host name of that computer (`austl1`) had been started and waiting to accept a connection.
Administrator opened another server with port number `51688` again.	A message "`Welcome to E-PAP Server! host = austl1 bind failed`" appeared, as port number `51688` had been opened.
Pressed `Ctrl + C`.	E-PAP Server stopped.

5.4.3 Phase III: Starting E-PAP Client

(Phase III was carried out by volunteers.)

Testing	Result
Logon without a server name	A message box alerted the user to provide a server name popup. (Figure 5-1)
Logon without a logon name	A message box alerted the user to provide a logon name popup. (Figure 5-2)
Logon without a server port number	A message box alerted the user to provide a port number popup. (Figure 5-3)
Logon with alphabet server port number	A message box alerted the user to provide a port number popup. (Figure 5-3)
Logon with a server port number less than 49152	As port number 0 to 1023 are reserved for well known ports, and 1024 to 49151 are registered ports, a message box alerted the user to provide a port number between 49152 to 65535 popup. (Figure 5-4)
Logon with a server port number more than 65535	A message box alerted the user to provide a port number between 49152 to 65535 popup. (Figure 5-4)
Logon with an invalid server name	A message box alerted the user to provide the correct server name or port number popup.

	(Figure 5-5)
Logon with invalid port number between 49152 to 65535	A message box alerted the user to provide a correct server name or port number popup. (Figure 5-5)
Tried to close E-PAP Client by clicking right mouse button and press close.	Right click mouse button had been disable and not allow to close E-PAP Client.
Tried to close E-PAP Client by pressing `Escape` key.	`Escape` key had been disable and not allow to close E-PAP Client.
Tried to close E-PAP Client by pressing `Alt + F4` key.	`Alt + F4` had been disable and not allow to close E-PAP Client.
Tried to close E-PAP Client by pressing `Ctrl + Alt + Del` and end task E-PAP Client.	`Ctrl + Alt + Del` had been disable and not allow to close E-PAP Client.
Tried to switch to other application by pressing `Alt + Tab`.	`Alt + Tab` had been disable and not allow to switch to other application.
Logon with server name `aust11` and port number `51688`.	Authentication process started (continue to Section 5.4.4).

Note: Testing in this phase did not consume any server kernel processing.

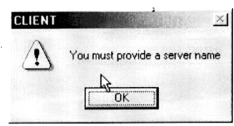

Figure 5-1: A message box alerted the user to provide a server name.

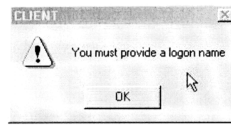

Figure 5-2: A message box alerted the user to provide a logon name.

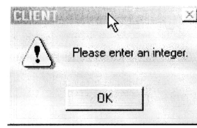

Figure 5-3: A message box alerted the user to provide a port number.

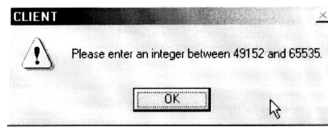

Figure 5-4: A message box alerted the user to provide a port number between 49152 to 65535.

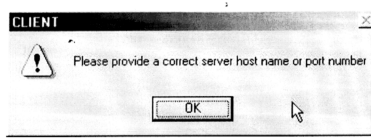

Figure 5-5: A message box alerted the user to provide correct server name or port number.

5.4.4 Phase IV: Starting Authentication

(Phase IV was carried out by volunteers.)

Testing	Result
Logon with logon name `test99` and password `Bo3jvmOj`.	A message box alerted the user about his / her logon name or password was wrong popup. (Figure 5-6) (Note: the correct logon name is `test01`) This failure was captured in E-PAP System Invalid User Log (`logxuser.txt`) with information: date, time, IP address, IP port and logon name. (Figure 5-7)
Logon with logon name `test01` and password `bOo3jvmOJ`.	A message box alerted the user about his / her logon name or password is wrong popup. (Figure 5-6) (Note: correct password is `Bo3jvmOj`) This failure was captured in E-PAP System Invalid Password Log (`logxpw.txt`) with information: date, time, IP address, IP port and logon name. (Figure 5-8)
Logon with logon name `test01` and password `Bo3jvmOj`.	A message box notified the user was verified and enquired the user to send message popup. (Figure 5-9) To prevent denial of service attack (DOS attack) that occupied E-PAP Server too long, this popup message will be closed automatically after 5 seconds if the user does not make a choice.
(continued from above) User wished to send message by clicking "OK" in Figure 5-9.	A dialog box popup to let user input messages (Figure 5-10). To prevent DOS attack, every message only given 60 seconds.

(continued from above) User sent the message by clicking "OK" in Figure 5-10.	The message had been sent without any disturbing from any third party. A message box notified the message had been successfully sent and required the user want to send other message again popup. (Figure 5-11). For more detail about this authenticated RPC, please refer to Figure 4-10.
(continued from above) User had sent three messages and wished to send an other message again.	A message box alerted the user that only maximum 3 messages was allowed popup (Figure 5-12). To prevent DOS attack, a user is only allowed to send a maximum of three messages.

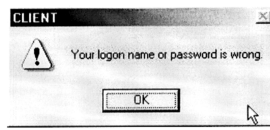

Figure 5-6: A message box alerted the user's logon name or password is wrong.

```
+--------------------------------+
| E-PAP System Invalid User Log |
+--------------------------------+

This is a log file to capture all invalid user logon name.
Please do not delete it.

NO     DATE          TIME          CLIENT IP      PORT   LOGON NAME
==     ====          ====          =========      ====   ==========
1.     2000-May-15   15:44:18      10.100.1.151   2308   test99
```

Figure 5-7: `logxuser.txt` file

```
+-----------------------------------+
| E-PAP System Invalid Password Log |
+-----------------------------------+

This is a log file to capture all invalid passwords.
Please do not delete it.

NO     DATE          TIME          CLIENT IP      PORT   LOGON NAME
==     ====          ====          =========      ====   ==========
1.     2000-May-15   15:56:03      10.100.1.151   2564   test01
```

Figure 5-8: `logxpw.txt` file

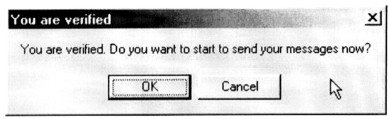

Figure 5-9: A message box notified the user is verified and enquire if the user want to send a message.

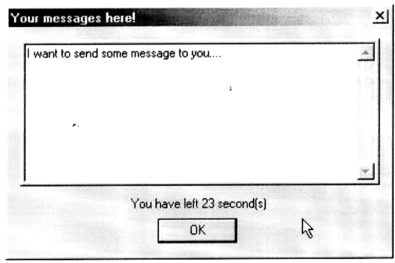

Figure 5-10: A dialog box for sending authenticated message.

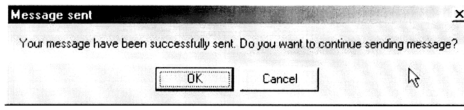

Figure 5-11: A message box notified the message has been successfully sent and enquire the user want to send other message again.

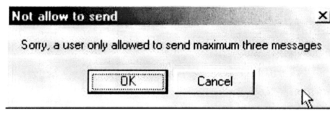

Figure 5-12: A message box alerted the user that only a maximum of 3 messages is allowed.

5.4.5 Phase V: Changing Password

(Phase V was carried out by voluntary participants.)

Testing	Result
Changed password by typing `Bo3jvmOj` in the new password field and `Bo3jvmOj` in the confirm password field. (Note: old password also is `Bo3jvmOj.`)	A message box alerted the user to provide other new password popup, as a new password is not allowed to be the same as old password. Both fields were then cleared. (Figure 5-13)
Changed password by typing `yctlck` in the new password field and `yctlck` in the confirm password field.	A message box alerted the user to provide new password with minimum eight characters popup. Both fields were then cleared. (Figure 5-14)
Changed password by typing `yctlckvm` in the new password	A message box alerted the user to re-input password popup, as new password field was not

field and `yctlckvM` in the confirm password field.	same as confirm password field (E-PAP password is case-sensitive). Both fields were then cleared. (Figure 5-15)
Changed password by typing `40226501` in the new password field and `40226501` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow numerical-only password. Both fields were then cleared. (Figure 5-16)
Changed password by typing `test01lck` in the new password field and `test01lck` in the confirm password field. (Note: Logon name field is `test01`)	A message box alerted the user to choose an other password popup, as E-PAP system does not allow a password to contain logon name. Both fields were then cleared. (Figure 5-17)
Changed password by typing `TEST01lck` in the new password field and `TEST01lck` in the confirm password field. (Note: Logon name field is test01)	A message box alerted the user to choose an other password popup, as E-PAP system does not allow a password to contain a logon name (regardless to case). Both fields were then cleared. (Figure 5-17)
Changed password by typing `10tsetlck` in the new password field and `10tsetlck` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain a reverse logon name. Both fields were then cleared. (Figure 5-17)
Changed password by typing `aaaayctl` in the new password field and `aaaayctl` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain 4 or more of same character (it is a bad chosen password). Both fields were then cleared.
Changed password by typing `yctlaaaa` in the new password field and `yctlaaaa` in confirm the password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain 4 or more of same character (it is a bad chosen password). Both fields were

	then cleared.
Changed password by typing `abcdefgh` in the new password field and `abcdefgh` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain 4 or more following ascending sequent characters (it is a bad chosen password). Both fields were then cleared.
Changed password by typing `AbCdEfGh` in the new password field and `AbCdEfGh` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain 4 or more following ascending sequent characters regardless to case (it is a bad chosen password). Both fields were then cleared.
Changed password by typing `hgfedcba` in the new password field and `hgfedcba` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain 4 or more following descending sequent characters (it is a bad chosen password). Both fields were then cleared.
Changed password by typing `HgFeDcBa` in the new password field and `HgFeDcBa` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain 4 or more following descending sequent characters regardless to case (it is a bad chosen password). Both fields were then cleared.
Changed password by typing `1234yctl` in the new password field and `1234yctl` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain 4 or more following ascending sequent numbers (it is a bad chosen password). Both fields were then cleared.
Changed password by typing `malaysia` in the new password field and `malaysia` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain word from dictionary. Both fields were then cleared. (Figure 5-18)

Changed password by typing `aisyalam` in the new password field and `aisyalam` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain reverse word from dictionary. Both fields were then cleared. (Note: `aisyalam` is reverse from `malaysia`) (Figure 5-18)
Changed password by typing `malaysia01` in the new password field and `malaysia01` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain word from dictionary. Both fields were then cleared. (Figure 5-18)
Changed password by typing `m4a0l32a2y6s5i0a` in the new password field and `m4a0l32a2y6s5i0a` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain word from dictionary. Both fields were then cleared. (Note: `m4a0l32a2y6s5i0a` contain `malaysia`) (Figure 5-18)
Changed password by typing `a4i0s2y2a615a0m` in the new password field and `a4i0s2y2a615a0m` in the confirm password field.	A message box alerted the user to choose an other password popup, as E-PAP system does not allow password to contain word from dictionary. Both fields were then cleared. (Note: `a4i0s2y2a6l5a0m` contain reverse word of `malaysia`) (Figure 5-18)
Changed password by typing `yctlckvm` in the new password field and `yctlckvm` in the confirm password field.	A message box notified user about password had been successfully changed popup. (Figure 5-19)

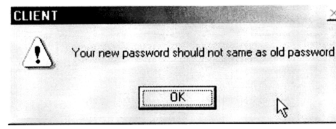

Figure 5-13: A message box alerted the user to provide other new password.

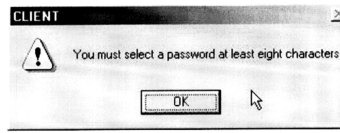

Figure 5-14: A message box alerted the user to provide new password with minimum eight characters.

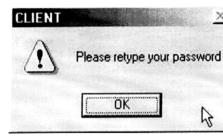

Figure 5-15: A message box alerted the user to re-input password.

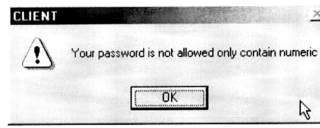

Figure 5-16: A message box alerted the user to choose an other password.

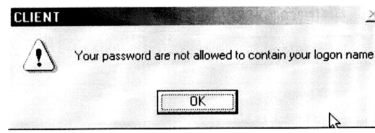

Figure 5-17: A message box alerted the user to choose an other password.

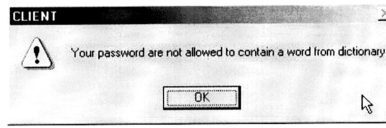

Figure 5-18: A message box alerted the user to choose an other password.

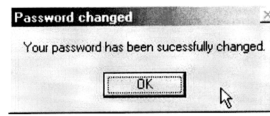

Figure 5-19: A message box notified user about password has been successfully changed.

5.4.6 Phase VI: Other Tests

Testing	Result
Client IP address `10.100.0.151` was added in `blockIP.txt` file manually by administrator. (Note: `10.100.0.151` was IP address for user `test01`)	A message notified user `test01` that he / she was blocked from server popup. (Figure 5-20)

During server process request from user `test01`, user `test02` connect to server.	User `test02` was accepted and idle until server finished process request from user `test01` as E-PAP Server is a single-thread server.
After server accepted 5 connections from user `test01`, `test02`, `test03`, `test04` and `test05`, user `test06` connect to server.	User `test06` was rejected from server as E-PAP Server only able to accept maximum 5 connections at a time.

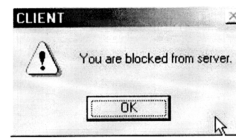

Figure 5-20: A message notified user that he / she was blocked from server.

5.5 *Discussion*

The results from the testing can prove that E-PAP System has fulfilled all strong authentication requirements that mentioned in Section 3.1.1 to 3.1.6. Section 5.5.1 to 5.5.6 showed the proof of each requirement.

5.5.1 Provide Mutual Authentication Without Revealing The Password

Mutual authentication requires each of two parties (Alice as E-PAP Client and Bob as E-PAP Server) to prove that it knows the password of the other. From Section 3.4.1, step 1 and 2 showed that

1. Alice computes: $Q_A = f(S)^{R_A} \bmod p$ $\quad A \rightarrow B: Q_A$
2. Bob computes: $Q_B = f(S)^{R_B} \bmod p$ $\quad B \rightarrow A: Q_B$

In Phase IV: Starting Authentication, Alice and Bob only can authenticate each other if they know the small shared password S. Note that both parties do not reveal its password to the other party, they only send an exponential value Q to each other. If Alice knows the password S, Bob convince her that he knows it too and vise-versa. In case Alice does not know the password, Bob does not reveal it. This achieves zero-knowledge mutual authentication.

5.5.2 Prevent Off-Line Dictionary Or Brute Force Attack

In Phase V: Changing Password, by using the same logon name and same password, the created credentials are not the same each time (refer to Table 5-2 and Table 5-3). This means user passwords are stored in a form that are not plaintext-equivalent to the password itself.

Table 5-2: Logon name, password and credential (1)

Logon Name	test01
Password	yctlckvm
Credential	s0028991F772DC0FE86032EAB16F1DE730FB7CF9769C9; S002820AC0B5D842049C1B466C7A9C6EFC398B54F222C; V0100575F5DF0F79E24BCD4EF2956480634CE63F4B6B81 CE4C52DCAE3A9B049B22DA0F34CDE57C91689DD7C8D95C ADB577DDE45DF437332BC25DE09A13F8B8AECE2FEE9918 97A95E6B6574F51B2A08501EED399EA35506C119B55F59 14B2FC216F4D9CACC1D4261C51E7C1868AA6904488A7F0 29156D24C4A01B7D8C9485E2FF04F7D;

Table 5-3: Logon name, password and credential (2)

Logon Name	test01
Password	yctlckvm
Credential	s0028F7629EEF091D057E3B2E3FE7CC52F1694E98F078; S00281A218086CAE25D87E02C30F07E4AC15EBA84EDBD; V0100814227CF3FAF75148777A8183FD2116A5CE8C6B8E CE4C52DCAE3A9B049B22DA0F34CDE57C91689DD7C8D95C

```
ADB577DDE45DF437332BC25DE09A13F8B8AECE2FEE9918
97A95E6B6574F51B2A08501EED399EA35506C119B55F59
14B2FC216F4D9CACC1D4261C51E7C1868AA6904488A7F0
29156D24C4A01B7D8C9485E2FF04F7D;
```

Therefore an attacker who captures the password database cannot use it directly to compromise security and gain immediate access to the host by applying off-line attack.

5.5.3 Prevent On-Line Dictionary And Brute-Force Attack

Table 2-2 shows that for a password with eight alphanumeric characters long, an offline attack may take 17 years to search for the correct password. For an online attack, the search time may increase to an order of one hundred thousand (1,700,000 years), which means E-PAP is theoretically unbreakable. Besides that, in Phase IV: Starting Authentication, any failed logon attempt due to invalid logon name and invalid password were captured in E-PAP System Invalid User Log (`logxuser.txt`) and E-PAP System Invalid Password Log (`logxpw.txt`) respectively. To prevent on-line dictionary and brute-force attack, an administrator can manually block any request from particular clients by adding that client IP address in `blockIP.txt` file.

5.5.4 Integrated Key Exchange

Strong key exchange requires the participation of both parties and should be an integral part of the process. In Phase IV: Starting Authentication, authentication and sending authenticated messages were integrated together (without separate the steps, attackers are not allowed to attack from the middle).

5.5.5 No Persistent Recorded Secret Or Sensitive Host-Specific Data

Unlike smartcard, E-PAP Client does not need additional symmetric, public or private (asymmetric) keys in all phases. All the credential files were stored on the

server side, this made the password as an independent factor. A smartcard requires a PKI or certification from a third party.

5.5.6 Forward Secrecy

Forward secrecy which involves revealing the password to an attacker does not help the attacker to obtain any information such as session keys of past sessions. In Phase IV: Starting Authentication, as session key K is a strong one-way hash function (SHA-1) of $Q^R \bmod p$ ($K = h(Q^R \bmod p)$) and $Q = f(S)^R \bmod p$, it is impossible to reverse this function. Therefore, stealing a session key K also does not help an attacker to carry out a brute-force attack on the password.

5.6 Strengths of E-PAP

5.6.1 Fulfill All Strong Authentication Requirements

E-PAP has fulfilled all strong authentication requirements which are mentioned in Section 3.1.1 to 3.1.6, which includes providing mutual authentication without revealing the password, prevent on-line and off-line dictionary / brute-force attack, integrated key exchange, no persistent recorded secret or sensitive host-specific data and forward secrecy. Besides that, E-PAP can be used in other environments discussed below.

5.6.2 Upgraded Existing Network Logon System

From Section 3.1 and 3.2, E-PAP has shown its strengths over many existing network logon system for various platforms. Therefore, E-PAP is suitable to be used to upgrade these vulnerable network logon systems. It also can be essential for new uses such as personal-computer remote banking or general computer logon over the Internet like Basic Authentication and Digest Authentication scheme [39].

5.6.3 Multi-Factor Authentication

Multi-factor authentication may be needed when neither a stored key nor a memorized password is strong enough. In a hybrid system, one should strive to make the password an independent factor, so that its security does not depend on persistent stored keys and vice-versa. Password-only methods can be combined with key-based method to build systems that can tolerate either a stolen password or a stolen key. A good example about multi-factor authentication is smarter-smartcard, which combines two of the three concepts of authentication, *something you have* (smartcard) and *something you know* (E-PAP).

5.6.4 Numeric-Keypad-Only System

In systems where only a numeric keypad is available, such as cellular telephone or phone banking authentication, a secure, short numeric password is especially convenient. TV remote-controlled set-top boxes might be another area of new applications [39].

5.6.5 Diskless Workstations

Diskless workstations like dump-terminal, is another class of device where it is inconvenient to have locally stored keys. Password-only methods are ideal for establishing an initial connection to a trusted host and to obtain the users safely stored credentials. This concept of remote storage of long-term credentials with a secure download has been used in the SPX authentication system [55].

5.6.6 Bootstrapping

Bootstrapping is the leveraging of a small initial effort into something larger and more significant. A bootstrap is a small strap or loop at the back of a leather boot that enables a administrator to pull the entire boot on. There is also a common expression, "pulling yourself up by your own bootstraps," meaning to leverage yourself to success from a small beginning [57]. The concept of bootstrapping to a new secure system is broad, and is best illustrated with a common case. An administrator is

installing a new network workstation from a CD-ROM. Somewhere during installation, he is prompted to enter a name and password to let him join the secure corporate network. Unless some additional site-specific keys are manually installed on the system, a strong password-only method is needed to allow the new station to make a secure channel to the rest of the network. Once an authenticated channel is established, the station can automatically obtain any further credentials or keys. Similar "bootstrapping" situations arise in almost all secure systems.

5.7 Limitations of E-PAP

5.7.1 Operating System Integration Problem

Unlike Linux that is publicly open and extensible by contributors, the kernel for Microsoft Windows family platform is not publicly open and extensible. Therefore, E-PAP system tries to execute before the original logon system, but not to fully replace the original logon system. After a user has successfully logon the E-PAP system with a correct logon name and password, he still have to logon with the original logon system to access to that network/computer. There is no solution for current time. All Windows user have no choice to switch from current logon system to E-PAP System, until Microsoft opens its kernel source code.

5.7.2 Single-threaded Server

This version of E-PAP Server is a single-threaded server. It can accept five connections simultaneously but only able to process one request from client at a time. As a result, to prevent a from user occupying the connection/channel too long and to prevent Denial-of-Service (DOS) attacks, an authenticated user is only allowed to send a maximum of three messages for a connection within sixty seconds for each message. The solution is to develop a multi-threaded server.