บรรณานุกรม

ภาษาอังกฤษ

Aho, Alfred V., Kernighan, Brian W., and Weinberger, Peter J. The Awk Programming Language Singapore: Addison-Wesley Publishing Co., 1986

Curry, David A. IMPROVING THE SECURITY OF YOUR UNIX SYSTEM [Machine-readable data file], Information and Telecommunications Sciences and Technology Division: SRI International, 1990

Farrow, Rik UNIX System Security : How to Protect Your Data and Prevent Intruders United States of America: Addison-Wesley Publishing Co., 1990

Garfinkel, Simson, and Spafford, Gene Practical UNIX Security United States of America: O'Reilly & Associates, Inc., 1991

Goodheart, Berny UNIX Curses Explained Australia: Prentice Hall of Australia Pty Ltd., 1991

Grampp, F.T. and Morris, R.H. "Unix Operating System Security," Unix System Readings and Applications Volume II pp.69-92, Prentice-Hall, 1987

Haviland, Keith, and Salama, Ben Unix System Programming Addison-Wesley Publishing Co., 1990

Hayes, Frank "Is Your System Safe ?", Unix World 6 (June 1990): 45-52

Morris, Robert, and Thompson, Ken "Password Security : A case history," UNIX Programmer's Manual , sec. 2, AT&T Bell Laboratories, 1984

Ritchie, Dennis M. "On the Security of UNIX," ULTRIX-32 Supplementary Documents Volume II System Managers . PP. 4-3-4-5, New Hampshire: Digital Equipment Corporation, 1984

Schreiner, Axel T. Using C with Curses,Lex and Yacc : building a window shell for UNIX System V Great Britain: Prentice Hall International, 1990

Wood, Patrick H., and Kochan, Stephen G. Unix System Security Sam Indianapolis Ind., 1988

ภาคผนวก

ภาคผนวก ก

รูปแบบของจอภาพ

โปรแกรมตรวจสอบความมั่นคงของระบบยูนิกซ์ ประกอบด้วย 8 จอภาพดังนี้

1. จอภาพเมนูหลัก
2. จอภาพตรวจสอบความมั่นคงของผู้ใช้
3. จอภาพตรวจสอบความมั่นคงของระบบ
4. จอภาพตรวจสอบความมั่นคงของเครือข่าย
5. จอภาพตรวจสอบความมั่นคงอื่นๆ
6. จอภาพตรวจสอบความมั่นคงของระบบ UUCP
7. จอภาพตรวจสอบความมั่นคงของ TCP/IP
8. จอภาพตรวจสอบความมั่นคงที่เกี่ยวข้องกับ SUID

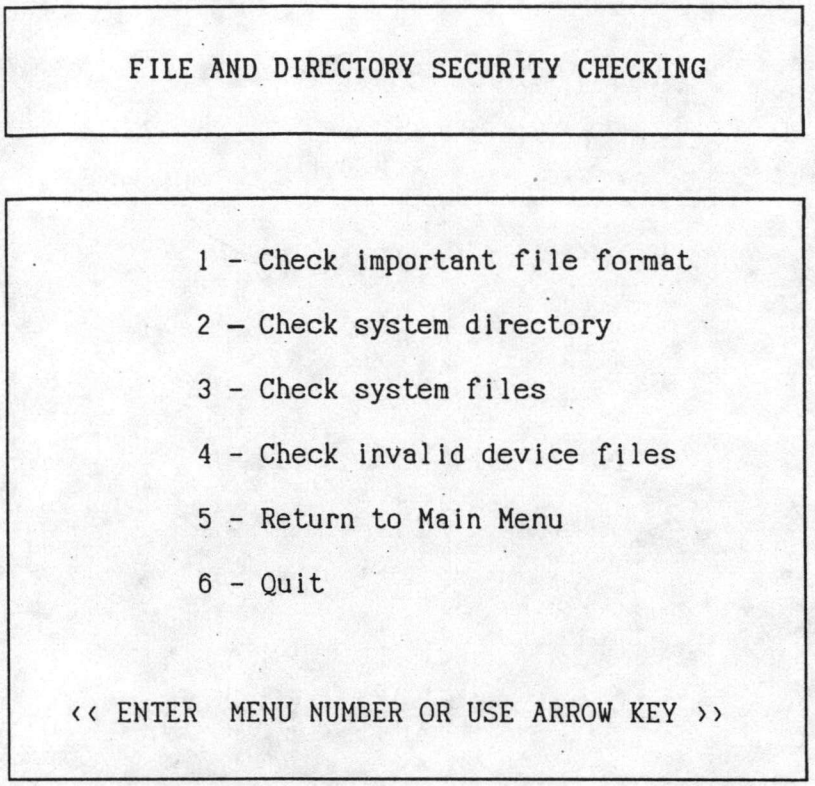
จอภาพเมนูหลัก

```
UNIX SECURITY CHECKING PROGRAM

        1 - User Directory
        2 - System Files and Directories
        3 - Networking
        4 - Miscellanous
        5 - Quit

<< ENTER  MENU NUMBER OR USE ARROW KEY >>
```

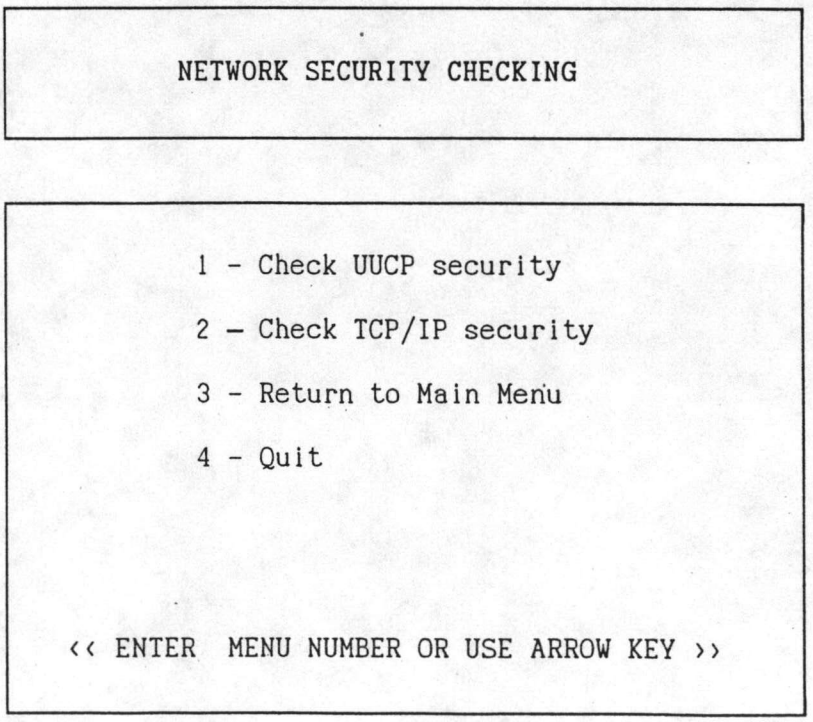
จอภาพตรวจสอบความมั่นคงของผู้ใช้

```
USER SECURITY CHECKING

        1 - Check improper search path
        2 - Check for improper permission
        3 - Check for possible trojan horse
        4 - Return to Main Menu
        5 - Quit

<< ENTER  MENU NUMBER OR USE ARROW KEY >>
```

จอภาพตรวจสอบความมั่นคงของระบบ



จอภาพตรวจสอบความมั่นคงของเครือข่าย



จอภาพตรวจสอบความมั่นคงอื่นๆ

```
        MISCELLANOUS  SECURITY CHECKING
```

```
            1 - Check mail directory permission
            2 – Check command and shell feature
            3 - Check intruding in root account
            4 - Check machine configuration
            5 - Check for invalid SUID and SGID
            6 - Return to Main Menu
            7 - Quit
    << ENTER  MENU NUMBER OR USE ARROW KEY >>
```

จอภาพตรวจสอบความมั่นคงของระบบ UUCP

```
        UUCP SECURITY CHECKING
```

```
            1 - Check important file permission
            2 – Return to Previous Menu
            3 - Return to Main Menu
            4 - Quit


    << ENTER  MENU NUMBER OR USE ARROW KEY >>
```

จอภาพตรวจสอบความมั่นคงของ TCP/IP

```
TCP/IP  SECURITY CHECKING

        1 - Check anonymous ftp
        2 – Check important file format
        3 - Check configuration file
        4 - Return to Previous Menu
        5 - Return to Main Menu
        6 - Quit

<< ENTER  MENU NUMBER OR USE ARROW KEY >>
```

จอภาพตรวจสอบความมั่นคงที่เกี่ยวข้องกับ SUID

```
SUID AND SGID SECURITY CHECKING

    1 - Check SUID and SGID in user directory
    2 – Check invalid SUID and SGID in system
    3 - Return to Previous Menu
    4 - Return to Main Menu
    5 - Quit

<< ENTER  MENU NUMBER OR USE ARROW KEY >>
```

ภาคผนวก ข

รูปแบบของการแสดงผล

ในภาคผนวกนี้ จะแสดงตัวอย่างการแสดงผลของชุดโปรแกรมตรวจสอบความมั่นคง โดยนำผลลัพธ์การแสดงผลมาจากเครื่อง MAMMOTH 386 และเครื่อง STAR SERVER

ตัวอย่างการแสดงผลจากโปรแกรม chkpath.sh

```
WARNING : gr1 has dangerous search path in .cshrc
WARNING : comp5 has dangerous search path in .profile
WARNING : pichai has dangerous search path in .login
```

ตัวอย่างการแสดงผลจากโปรแกรม chkuser.sh

```
Check user's home directory in progress ...

WARNING : User "thong" has .rhosts
WARNING : User "oracle" has writable directory for other
WARNING : User "wichai" has writable directory for other
WARNING : User "atp" has .rhosts
WARNING : User "comp1"  has writable directory for other
WARNING : User "comp2"  has writable directory for other
```

ตัวอย่างการแสดงผลจากโปรแกรม trojan.sh

```
Checking for possible trojan horse in progress ...

WARNING : Possible trojan horse in /usr2/gr1/ps
WARNING : Possible trojan horse in /usr2/thong/mks/vi
WARNING : Possible trojan horse in /usr2/woot/ps
```

ตัวอย่างการแสดงผลจากโปรแกรม passwd.sh

```
Checking permission in /etc/passwd ...
Permission for /etc/passwd O.k.
Checking for invalid entry in /etc/passwd ...
Done

Checking permission in /etc/group ...
Permission for /etc/group O.k.
Checking for invalid entry in /etc/group ...
Done

Checking permission in /etc/shadow ...
WARNING : Invalid permission in /etc/shadow
-r--r--r--
Checking for invalid entry in /etc/shadow ...
WARNING :Account nuucp does not have password
WARNING :Account sync does not have password
WARNING :Account rteew does not have password

Checking /etc/inittab in progress ...
Done
```

ตัวอย่างการแสดงผลจากโปรแกรม checkdir.sh

```
Check world-writable directory under /bin ...

Check world-writable directory under /etc ...
WARNING :These directory under /etc have world-writable mode
        /etc/conf/pack.d/xi
        /etc/rc0.d
        /etc/rc2.d

Check world-writable directory under /usr ...
WARNING :These directory under /usr have world-writable mode
        /usr/adm/logbook
        /usr/include/sys
        /usr/include/net
        /usr/lbin/etc
        /usr/vpix/etc
        /usr/oracle/forms/man
        /usr/oracle/menu/man

Check world-writable directory under /lib ...
WARNING :These directory under /lib have world-writable mode
        /lib/cftime
        /lib/chrclass
```

ตัวอย่างการแสดงผลจากโปรแกรม checkfile.sh

```
Check world-writable files under /bin ...

Check world-writable files under /etc ...
WARNING :These files under /etc have world-writable mode
         /etc/conf/init.d/si

Check world-writable files under /usr ...
WARNING :These files under /usr have world-writable mode
         /usr/lib/INSTALL.USR
         /usr/spool/lp/logs/lpsched

Check world-writable files under /lib ...
```

ตัวอย่างการแสดงผลจากโปรแกรม uucp.sh

```
Home directory of uucp account is /usr/lib/uucp
nuucp account has home directory in /usr/spool/uucppublic
Your machine have usrida as uucp users

Checking UUCP related commands in progress ...
Your machine does not have uuencode program
WARNING :/usr/bin/cu has improper owner
WARNING :/usr/bin/uuto has improper owner

Checking /usr/lib/uucp in progress ...
WARNING :Your machine does not have file uudemon.deny
```

ตัวอย่างการแสดงผลจากโปรแกรม tcpfile.sh

```
Checking /etc/hosts file format in progress ...

Checking /etc/hosts.equiv file format in progress ...
WARNING :"+" exist in /etc/hosts.equiv

Checking  /etc/services file format in progress ...

Checking /etc/inetd.conf file format in progress ...
WARNING :Shell /bin/ksh is in /etc/inetd.conf as /usr/bin/ksh
```

ตัวอย่างการแสดงผลจากโปรแกรม tcpchk.sh

```
Check security in tftp command in progress ...
Your /usr/bin/tftp is O.k.

Checking sendmail program in progress ...
Trying 127.0.0.1 (Port 25) ...
Connected to localhost.chula.ac.th
220 chulkn.chula.ac.th Smail 3.1.28 #12 Ready at Mon,3 May 93
11:31 BKK
500 Command unrecognized
250 Debugging level:1
500 Command unrecognized
221 chulkn.chula.ac.th closing connection
connection closed.
If it display message other than "Command unrecognized" ,
replace your sendmail
```

ตัวอย่างการแสดงผลจากโปรแกรม chkmail.sh

```
Checking mail directory in progress ...
Your mail directory is /usr/mail

WARNING :/usr/mail has invalid group name
WARNING :/usr/mail/compl has write permission for other
WARNING :/usr/mail/grl has invalid owner name
WARNING :/usr/mail/pichai has read permission for other
```

ตัวอย่างการแสดงผลจากโปรแกรม chkmisc.sh

```
WARNING :write command has improper permission

Your preserve program is /usr/lib/expreserve
WARNING :/usr/lib/expreserve has improper mode

Checking find command  : o.k.
Checking shell command : o.k.
Checking xargs command : o.k.
Checking IFS feature   : o.k.
```

ตัวอย่างการแสดงผลจากโปรแกรม sulog.sh

```
WARNING :/usr/adm/sulog has invalid permission mode

Enter user name 1 who can login as root : fyta
Enter user name 2 who can login as root : thong
Enter user name 3 who can login as root :

Scanning /usr/adm/sulog for unauthorized user .....

WARNING :"guest" broken to root account !!!
WARNING :"gr1" broken to root account !!!
```

ตัวอย่างการแสดงผลจากโปรแกรม config.sh

```
Checking format in file /usr/default/su in progress ...
su logging file is /usr/adm/sulog
When use su command , it will not display on console

Checking format in file /etc/default/login ...
Maximum file size is 2048 Mega Byte

user root can login at any terminal
Any user is not required to have password
```

ตัวอย่างการแสดงผลจากโปรแกรม suid1.sh

```
Enter directory you want to search : /usr2

Checking SUID and SGID files under /usr2 in progress ...

WARNING :/usr2/guest/badsh is SUID file
WARNING :/usr2/pichai/manx is SGID file
WARNING :/usr2/thong/bin/chkuser is SUID file
```

ตัวอย่างการแสดงผลจากโปรแกรม suid2.sh

```
Checking for invalid SUID and SGID files in progress ...

WARNING :These are invalid SUID and SGID files
         /usr/lib/osh
         /usr/oracle/bin/oracle0
         /usr2/guest/badsh
         /usr2/pichai/manx
         /usr2/thong/bin/chkuser
```

ประวัติผู้เขียน

นายธงชัย โรจน์ก้งสดาล เกิดเมื่อวันที่ 12 พฤศจิกายน พ.ศ. 2509 ที่กรุงเทพมหานคร สำเร็จการศึกษาระดับปริญญาตรีวิศวกรรมศาสตร์บัณฑิต จากภาควิศวกรรมสำรวจ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2530 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตร์มหาบัณฑิต สาขาวิทยาศาสตร์คอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อ พ.ศ. 2531 ในระหว่างศึกษาได้รับทุนจากมูลนิธิเพื่อการศึกษาคอมพิวเตอร์และการสื่อสาร และทุนผู้ช่วยสอนของบัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย ตามลำดับ