CXL SECURE

AZScan

Report for
Demo

07-Dec-2008 19:53

Report for	Demo
Company	CXL Finance
Business Unit	Finance Division
Location	London
System	FINSYS202

Report Name	c:\tbxnew-works\reports\myrepv.doc
Report Date	07-Dec-2008 19:53

Key to colors

Risks	L Low risk	M Medium risk	H High risk
Results	L Correct or low risk	M Medium impact	H Major problem

1 SUMMARYSummary

1.1	PRIVS	H Privileges	H 14high users.
1.2	LEVELS	H Levels	L Level 0 - 0 Level 1 - 0 Level 2 - 0 Level 3 - 48 Level 4 - 4 Level 5 - 0 Level 6 - 10
1.3	FLAGS	H Flags	L -
1.4	NETLI	M Network Logins	M -

2 PWDSPasswords

2.1	PWDLIFE	M Password life	M 91 days.
2.2	PWDLIFESTD	M Password life vs. standards	H 26
2.3	PWDCHANGES	M Distribution of password changes	H 170 average days.
2.4	PWDLEN	M Password length	L 6 chrs.
2.5	PWDLENSTD	M Password length vs. standards	H 23

3 A/CAccounts

3.1	UNA/C	M Unused accounts	M 10
3.2	NOOWN	L No owners	M 12

4 SPACSpecific accounts

4.1	AC-SYSTEM	H SYSTEM Account	L Done
4.2	AC-FIELD	H FIELD Account	L Done
4.3	AC-DEFAULT	H DEFAULT Account	L Done

5 LOGINSLogins

5.1	LINOI	L Non-interactive Logins	L 2
5.2	LIBOT	L Both types of login	L 5
5.3	LIINT	L Interactive logins	L 44
5.4	LLOGINS	L Last logins	M 99 days.
5.5	LIFAIL	L Login failures	H 15 users.
5.6	DEFDIR	L Default Directories	L 5 users.
5.7	CLI	L CLI	M 21 users.

5.8	LGICMD	L LGICMD	H 15 users.
5.9	NCAPTIVE	M Non-Captive	M 10 users.

6 UICSUICs

6.1	SHUICS	M Shared UICs	M 8 UICs
6.2	LOWUICS	M Low value UICs	H 13

7 SYSSETSystem settings

7.1	UNLCPU	M Unlimited cpu	L 0
7.2	PRCLM	L PRCLM	L 0
7.3	MXDETACH	M Max Detached	M 58

8 FLAGSFlags

8.1	CAPTIVE	L Captive	L 52 users.
8.2	DISWELCOME	M Diswelcome	L 0 users.
8.3	DISNEWMAIL	L Disnewmail	L 0 users.
8.4	DISMAIL	L Flag - Dismail	H 4 users.
8.5	GENPWD	M Flag - Genpwd	L 0 users.
8.6	DISIMAGE	L Flag - Disimage	H 0 users.
8.7	DISRECONNECT	L Flag - Disreconnect	H 0 users.
8.8	DISREPORT	H Flag - Disreport	L 0 users.
8.9	DISUSER	L Flag - Disuser	L 6 users.
8.10	LOCKPWD	M Flag - Lockpwd	L 4 users.
8.11	PWD_EXPIRED	L Flag - Pwd_expired	L 0 users.
8.12	RESTRICTED	L Flag - Restricted	L 47 users.
8.13	DISPWDDIC	M Flag - Dispwddic	H 61 users.
8.14	DEFCLI	M Flag - Defcli	H 0 users.
8.15	DISCTLY	L Flag - Disctly	L 48 users.
8.16	AUDIT	L Flag - Audit	L 2 users.
8.17	AUTOLOGIN	L Flag - AutoLogin	L 0 users.
8.18	DISFORCE_PWD_CHANGE	M Flag - Disforce_pwd_change	L 0 users.
8.19	DISPWDHIS	M Flag - Dispwdhis	L 0 users.
8.20	PWD2_EXPIRED	L Flag - Pwd2_Expired	L 3 users.
8.21	EXTAUTH	L Flag - External authentication	L 0 users.
8.22	VMSAUTH	L Flag - VMSauth	L 0 users.
8.23	PWDMIX	M Flag - PwdMix	L 2 users.
8.24	DISPWDSYNCH	L Flag - DisPwdSynch	L 3 users.

9 LEVELSLevels

9.1	LEVELS4-6	H Levels 4 to 6	H 14 users.

10 PRIVSPrivileges

10.1	ACNT	L Privilege - Acnt	L 1 users.
10.2	ALLSPOOL	L Privilege - Allspool	L 1 users.
10.3	ALTPRI	M Privilege - Altpri	L 2 users.
10.4	BUGCHK	M Privilege - BugChk	L 2 users.
10.5	BYPASS	M Privilege - ByPass	H 5 users.
10.6	CMEXEC	L Privilege - Cmexec	L 1 users.

10.7	CMKRNL	M Privilege - Cmkrnl	M 2 users.
10.8	DETACH	L Privilege - Detach	L 1 users.
10.9	DIAGNOSE	L Privilege - Diagnose	L 1 users.
10.10	EXQUOTA	L Privilege - Exquota	L 1 users.
10.11	GROUP	L Privilege - Group	L 1 users.
10.12	GRPNAM	L Privilege - Grpnam	L 1 users.
10.13	GRPPRV	L Privilege - Grpprv	L 1 users.
10.14	LOGIO	L Privilege - LogIO	M 2 users.
10.15	MOUNT	M Privilege - Mount	L 1 users.
10.16	NETMBX	L Privilege - Netmbx	L 1 users.
10.17	OPER	M Privilege - Oper	M 12 users.
10.18	PFNMAP	L Privilege - Pfnmap	L 1 users.
10.19	PHYIO	M Privilege - Phyio	M 2 users.
10.20	PRMCEB	L Privilege - Prmceb	L 2 users.
10.21	PRMGBL	L Privilege - Prmgbl	L 2 users.
10.22	PRMMBX	L Privilege - Prmmbx	L 2 users.
10.23	PSWAPM	L Privilege - Pswapm	L 1 users.
10.24	READALL	H Privilege - Readall	H 4 users.
10.25	PSECY	H Privilege - Security	L 2 users.
10.26	SETPRV	M Privilege - Setprv	M 2 users.
10.27	SHARE	L Privilege - Share	L 1 users.
10.28	SHMEM	L Privilege - Shmem	L 1 users.
10.29	SYSGBL	M Privilege - Sysgbl	L 1 users.
10.30	SYSLCK	M Privilege - Syslck	L 1 users.
10.31	SYSNAM	H Privilege - Sysnam	M 2 users.
10.32	SYSPRV	H Privilege - Sysprv	M 3 users.
10.33	TMPMBX	L Privilege - Tmpmbx	L 3 users.
10.34	VOLPRO	L Privilege - Volpro	M 2 users.
10.35	WORLD	L Privilege - World	L 2 users.
10.36	AUDIT	M Privilege - Audit	L 1 users.
10.37	DGRADE	M Privilege - Downgrade	L 1 users.
10.38	PIMPT	L Privilege - Import	L 1 users.
10.39	UGRADE	L Privilege - Upgrade	L 1 users.
10.40	IPNATE	M Privilege - Impersonate	M 3 users.
10.41	OVERALL	M Flags/Privilege - Overall	L -

1 SUMMARY - Summary

RISKS

The following sections summarise the key areas of this review.

1.1 PRIVS - Privileges

H

RISKS

Privileges determine what a user can and cannot do on a system. They determine what processes will work for a user.
The most important privileges are the ones which permit the user to run the AUTHORIZE program which then enables them to create accounts with whatever privileges they wish.
Such an account will have full access to all the data, software and even the logs recording the activity of the users.

ACTIONS

With these privileges a user can do anything to your system and cover their tracks. Privileges at or above level 4 fall into this category.

H

RESULTS

Number of users with the following privileges:

Level	Privilege	No.	%
1	Mount	1	2
1	Netmbx	62	100
1	Tmpmbx	62	100
2	Group	62	100
2	Grpprv	1	2
3	Acnt	1	2
3	Allspool	1	2
3	Bugchk	0	0
3	Exquota	1	2
3	Grpnam	62	100
3	Prmceb	2	3
3	Prmgbl	0	0
3	Prmmbx	2	3
3	Shmem	1	2
4	Altpri	2	3
4	Oper	12	19
4	Pswapm	1	2
4	Security	2	3
4	Syslck	1	2
4	World	2	3
4	Audit	1	2
5	Diagnose	1	2
5	Sysgbl	0	0
5	Volpro	2	3
5	Import	0	0
6	Bypass	5	8
6	Cmexec	1	2
6	Cmkrnl	2	3
6	Detach	1	2
6	Log_IO	2	3
6	Pfnmap	1	2
6	Phy_IO	2	3
6	Readall	4	6
6	Setprv	2	3
6	Share	1	2
6	Sysnam	2	3
6	Sysprv	3	5
6	Downgrade	0	0
6	Upgrade	0	0
6	Impersonate	3	5

1.2 LEVELS - Levels

H

RISKS

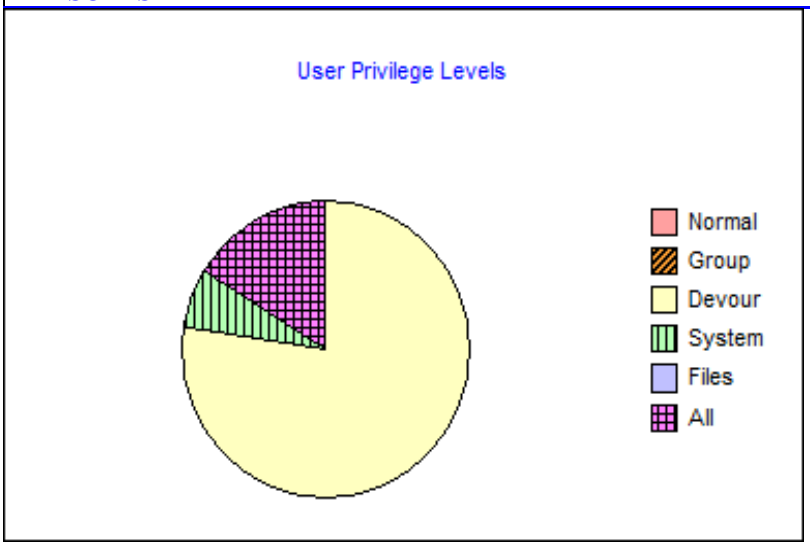
Each of the privileges shown previously has been categorised into 7 levels (0-6).
These are in order of the 'damage' they are capable of doing to a system.

ACTIONS

Users at levels 4 to 6 are considered to be dangerous and the number of such accounts should be strictly limited.We would not expect to see more than about 7 accounts at these levels.

L

RESULTS



Number of users at each level:

Level	Name	No.	%
0	None	0	0
1	Normal	0	0
2	Group	0	0
3	Devour	48	77
4	System	4	6
5	Files	0	0
6	All	10	16

1.3 FLAGS - Flags

H

RISKS

A section of the SYSUAF record details the flags set for each user. Flags, like privileges, limit the facilities available to a user. In general, they tend to prevent users doing certain actions or receiving certain information.

ACTIONS

Examine the flags set for users and ensure that they are appropriate.

L

RESULTS

```
Number of users with the following flags set:

Flag                         No.      %
---------------------------------------
NONE                          0       0
Captive                      52      84
Diswelcome                    0       0
Disnewmail                    0       0
Dismail                       4       6
Genpwd                        0       0
Disimage                      0       0
Disreconnect                  0       0
Disreport                     0       0
Disuser                       6      10
Lockpwd                       4       6
Ppwd_expired                  0       0
Restricted                   47      76
Dispwddic                    61      98
Defcli                        0       0
Disctly                      48      77
Audit                         2       3
Autologon                     0       0
Disforce_pwd_change           0       0
Dispwdhis                     0       0
Pwd2_expired                  3       5
ExtAuth                       0       0
VMSAuth                       0       0
PwdMix                        2       3
DisPwdSynch                   3       5
```

1.4 NETLI - Network Logins

M

RISKS

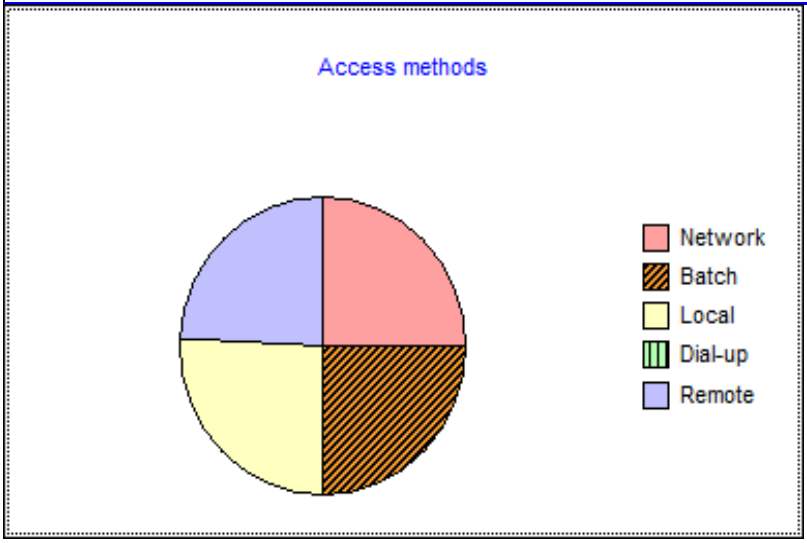
A NETWORK login is usually made to your system by a user doing a remote file access to it using DECNET. Many DCL commands specify a file or operation which can be performed across DECNET. They are non-interactive.
A BATCH login occurs when a user runs a batch job on the system using SUBMIT.
A LOCAL login is one that occurs from a terminal that is connected directly to the computer, or is on a Local Area Network and has CONNECT access to it. LOCAL logins are always interactive.
A DIALUP login is one that occurs from a terminal connected to a telephone line via a modem. If LOGINOUT sees that the line has the permanent characteristic /DIALUP, it automatically classifies the login as DIALUP. The most secure systems do not have ANY dial-up lines. If your system MUST have some form of dial-up, then VMS provides you with some security tools which counter someone trying to guess a password on your system over a dial-up line, and make dialling-in easier for authorised users.
A REMOTE login is made to your system by a remote user typing the command:
o $ SET HOST
This causes DECNET, to make a connection between them. If the node is reachable, the login sequence will be interactive.

ACTIONS

Examine the numbers of users in each category and ensure that it is appropriate.Dialup access is frequently given without good reason.

M

RESULTS



Number of users with different methods of access:

Method	No.	%
Network	44	71
Batch	44	71
Local	46	74
Dial-up	0	0
Remote	43	69

2 PWDS - Passwords

RISKS

To list the users without passwords you need to issue this DCL instruction:
uaf/sel=password="/display=(user)
This will list all users without passwords.

2.1 PWDLIFE - Password life

M

RISKS

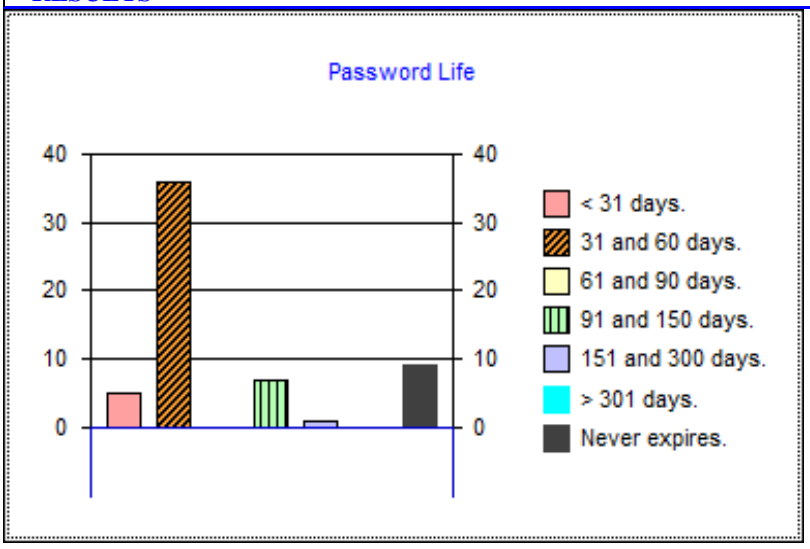
The default length of time that a password is usable before it has to be changed.
EVERY account should have a password life set.
A password which is not changed frequently can become widely known.

ACTIONS

We consider 90 days to be too long for most commercial systems and we would recommend 30 days.Thus any passwords with a life of longer than 60 days should be changed immediately.

M

RESULTS



Distribution of password lifetimes.

Password never expires.

CXL_PJM		Never
CXL_SYSTEM	GENERAL SYSTEM X	Never
DEFAULT	GGM DEFAULT	Never
GEN_PJM		Never
GEN_SYSTEM	GENERAL SYSTEM	Never
GGM_TRAIN1	TRAINING 1	Never
SYSTEM	SYSTEM MANAGER	Never
XGM_DEFAULT	XGM DEFAULT BT	Never
XGM_TRAIN1	TRAINING 1X	Never

Users in this range = 9 (15%)

Password life greater than 301 days.

No users fall into this range.

Password life between 151 and 300 days.

CXL_JMM	J. MOLESON	235 days.

Users in this range = 1 (2%)

Password life between 91 and 150 days.

CXL_AFT		99 days.
CXL_JMJC		135 days.
CXL_PT	P.TELLY	135 days.
GEN_PM	DEP - P.SMITH	99 days.
YGEN_PM	DEP - P.SMITH	99 days.
ZEN_PM	DEP - P.SMITH	99 days.
ZZN_PM	DEP - P.SMITH	99 days.

Users in this range = 7 (11%)

Password life between 61 and 90 days.

No users fall into this range.

Password life between 31 and 60 days.

CXL_AGS		35 days.
CXL_AJL		35 days.
CXL_BG	DEP - B.GOLDS	35 days.
CXL_BGL		35 days.
CXL_BPB	B.P.BROWN	35 days.
CXL_JC	IBM - J.COOPER	35 days.
CXL_JHM	J.H.MARTIN	35 days.
CXL_JLP	J. PETERS	35 days.
CXL_JMH	J. HOWELL	35 days.
CXL_JMI	J. IVY	35 days.
CXL_JML	J. LEADBETTER	35 days.
CXL_JMN	J. NORTON	35 days.
CXL_JNM		35 days.
CXL_JO	J.OXSHOT	35 days.
CXL_JPC	J.P.CROMPTON	35 days.
CXL_JPJ		35 days.
CXL_JPL	J. LENT	35 days.
CXL_JRD	J. ROVER	35 days.
CXL_JS	J.SMILEY	35 days.
CXL_JTH	J. HARRY	35 days.
CXL_MDM	M.D.MANTA	35 days.
CXL_MEZ	M.E.ZENT	35 days.
CXL_MJC	M.J.COLLINS	35 days.
CXL_MKB	M.K.BROWN	35 days.
CXL_MLW	M.WEBSTER	35 days.
CXL_MNH	M.N.HUNTER	35 days.

2.2 PWDLIFESTD - Password life vs. standards

M

RISKS

Company standards are not being applied to these users.
We recommend that passwords for 'system' users should be set to 30 days or less and for 'ordinary' users, it should be set to 60 days or less.

ACTIONS

Set password life times to your company standards.

H

RESULTS

The following 'system' users have password lifetimes below your company standards.

User		Life	Std
CXL_AJL		35	30
CXL_BPB	B.P.BROWN	35	30
CXL_JMJC		135	30
CXL_JML	J. LEADBETTER	35	30
CXL_JPJ		35	30
CXL_JPL	J. LENT	35	30
CXL_MKB	M.K.BROWN	35	30
CXL_PJM		None	30
CXL_PRN		35	30
CXL_PRT	TNT_OPER2	35	30
CXL_RT	R.TULL	35	30
CXL_SYSTEM	GENERAL SYSTEM X	None	30
GEN_PJM		None	30
GEN_SYSTEM	GENERAL SYSTEM	None	30
SYSTEM	SYSTEM MANAGER	None	30

15'system' users do not have a password life of at least 30 days.

The following 'ordinary' users have password lifetimes below your company standards.

User		Life	Std
CXL_AFT		99	60
CXL_JMM	J. MOLESON	235	60
CXL_PT	P.TELLY	135	60
DEFAULT	GGM DEFAULT	None	60
GEN_PM	DEP - P.SMITH	99	60
GGM_TRAIN1	TRAINING 1	None	60
XGM_DEFAULT	XGM DEFAULT BT	None	60
XGM_TRAIN1	TRAINING 1X	None	60
YGEN_PM	DEP - P.SMITH	99	60
ZEN_PM	DEP - P.SMITH	99	60
ZZN_PM	DEP - P.SMITH	99	60

11'ordinary' users do not have a password life of at least 60 days.

2.3 PWDCHANGES - Distribution of password changes

M

RISKS

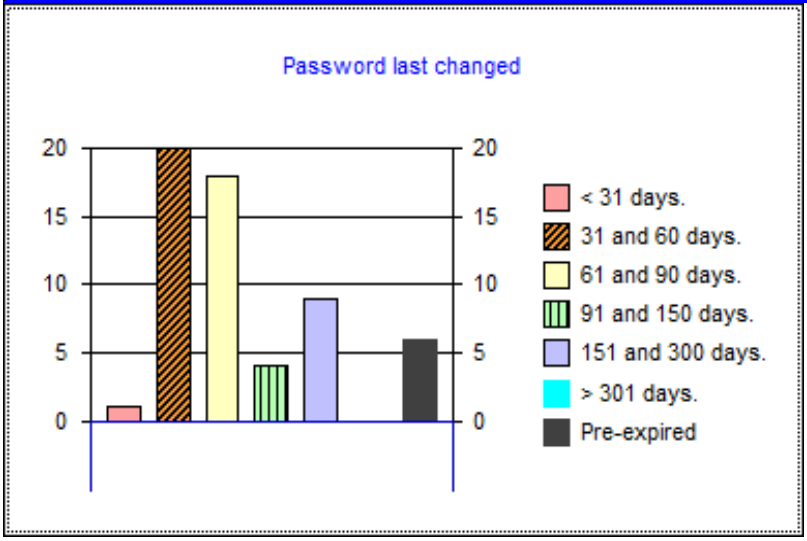
Detailed below are the times when the users' passwords were last changed.
A password may be set to PRE-EXPIRED and when a user first logs on they will be forced to change it. The system behaves as if the password had reached its expiration date.
A password which is not changed frequently can become widely known.

ACTIONS

Any passwords which have not been changed for a long time either belong to accounts which have a long password expiry set (reduce it) or the account has not been used for a long time (delete it).

H

RESULTS



Distribution of password changes.

Password pre-expired.

CXL_AGS		Pre-expired
CXL_AJL		Pre-expired
CXL_BPB	B.P.BROWN	Pre-expired
CXL_MNH	M.N.HUNTER	Pre-expired
DEFAULT	GGM DEFAULT	Pre-expired
XGM_DEFAULT	XGM DEFAULT BT	Pre-expired

Users in this range = 6 (10%)

Password changed more than 301 days.

No users fall into this range.

Password changed between 151 and 300 days.

CXL_BGL		297 days.
CXL_JHM	J.H.MARTIN	266 days.
CXL_JPC	J.P.CROMPTON	251 days.
CXL_MDM	M.D.MANTA	239 days.
CXL_MJC	M.J.COLLINS	192 days.
CXL_MLW	M.WEBSTER	152 days.
CXL_RET	R.TAYLOR	186 days.
CXL_RH		153 days.
GEN_PJM		166 days.

Users in this range = 9 (15%)

Password changed between 91 and 150 days.

CXL_JMS	J. SMITH	111 days.
CXL_NH	N.HOWELL	141 days.
CXL_PJM		135 days.
CXL_SYSTEM	GENERAL SYSTEM X	117 days.

Users in this range = 4 (6%)

Password changed between 61 and 90 days.

CXL_AFT		64 days.
CXL_BG	DEP - B.GOLDS	70 days.
CXL_JC	IBM - J.COOPER	67 days.
CXL_JML	J. LEADBETTER	64 days.
CXL_JNM		64 days.
CXL_JO	J.OXSHOT	62 days.
CXL_JPJ		69 days.
CXL_MC	DEP - M.COOL	68 days.
CXL_PS		64 days.
CXL_RT	R.TULL	69 days.
GEN_MC	DEP - M.COLLINS	68 days.
GEN_PM	DEP - P.SMITH	61 days.
GEN_SYSTEM	GENERAL SYSTEM	86 days.
GGM_TRAIN1	TRAINING 1	61 days.
SYSTEM	SYSTEM MANAGER	62 days.
XGM_TRAIN1	TRAINING 1X	61 days.
ZEN_PM	DEP - P.SMITH	61 days.
ZZN_PM	DEP - P.SMITH	61 days.

Users in this range = 18 (29%)

Password changed between 31 and 60 days.

CXL_JLP	J. PETERS	43 days.
CXL_JMH	J. HOWELL	43 days.
CXL_JMI	J. IVY	48 days.
CXL_JMJC		55 days.
CXL_JMM	J. MOLESON	43 days.
CXL_JMN	J. NORTON	48 days.

2.4 PWDLEN - Password length

M

RISKS

This is the minimum length required for a user's password.
Short passwords are easy to guess.

ACTIONS

We recommend that passwords are at least 6 characters in length. Any shorter and they become too easy to guess. Much past 8 characters and users will tend to write them down. You may consider it beneficial for 'system' accounts to have passwords of at least 8 characters.

L

RESULTS

```
Users with min. password length= 0
CXL_MC          DEFAULT         GEN_MC          XGM_DEFAULT
 4 users.


Users with min. password length= 2
CXL_JTH         GEN_PM
 2 users.


Users with min. password length= 3
CXL_JMM         CXL_SYSTEM      GEN_SYSTEM
 3 users.


Users with min. password length= 6
CXL_AFT         CXL_AGS         CXL_AJL         CXL_BG          CXL_BGL
CXL_BPB         CXL_JC          CXL_JHM         CXL_JLP         CXL_JMH
CXL_JMI         CXL_JMJC        CXL_JML         CXL_JMN         CXL_JMS
CXL_JNM         CXL_JPC         CXL_JPJ         CXL_JPL         CXL_JRD
CXL_JS          CXL_MDM         CXL_MEZ         CXL_MJC         CXL_MKB
CXL_MLW         CXL_MNH         CXL_NH          CXL_NJM         CXL_PAC
CXL_PJM         CXL_PJR         CXL_PM          CXL_PRN         CXL_PRT
CXL_PS          CXL_PT          CXL_RET         CXL_RH          CXL_RT
FIELD           GEN_PJM         GGM_TRAIN1      XGM_TRAIN1
 44 users.


Users with min. password length= 8
SYSTEM
 1 users.


Users with min. password length= 9
YGEN_PM         ZEN_PM          ZZN_PM
 3 users.


Users with min. password length= 44
CXL_JO
 1 users.
```

2.5 PWDLENSTD - Password length vs. standards

M

RISKS

Shown here are users with passwords below your company standards.

ACTIONS

We recommend that passwords are at least 6 characters in length. Any shorter and they become too easy to guess.Longer than 8 characters and 'ordinary'users will tend to write them down.You may consider it beneficial for 'system' accounts to have passwords of at least 8 characters.

(H)

RESULTS

The following 'system' users have password lifetimes below your company standards.

User		Life	Std
CXL_AJL		6	8
CXL_BPB	B.P.BROWN	6	8
CXL_JMJC		6	8
CXL_JML	J. LEADBETTER	6	8
CXL_JPJ		6	8
CXL_JPL	J. LENT	6	8
CXL_MC	DEP - M.COOL	0	8
CXL_MKB	M.K.BROWN	6	8
CXL_NJM	N.J.MILTON	6	8
CXL_PJM		6	8
CXL_PRN		6	8
CXL_PRT	TNT_OPER2	6	8
CXL_RT	R.TULL	6	8
CXL_SYSTEM	GENERAL SYSTEM X	3	8
FIELD	FIELD	6	8
GEN_MC	DEP - M.COLLINS	0	8
GEN_PJM		6	8
GEN_SYSTEM	GENERAL SYSTEM	3	8

18'system' users do not have a password length of at least 8 chrs.

The following 'ordinary' users have password length below your company standards.

User		Len	Std
CXL_JMM	J. MOLESON	3	6
CXL_JTH	J. HARRY	2	6
DEFAULT	GGM DEFAULT	0	6
GEN_PM	DEP - P.SMITH	2	6
XGM_DEFAULT	XGM DEFAULT BT	0	6

5'ordinary' users do not have a password length of at least 6 chrs.

3 A/C - Accounts

RISKS

This section reviews the users' accounts for specific problems. Problems may be trivial in themselves but when combined with some of the other problems or facilities available to a user, may become very significant.

3.1 UNA/C - Unused accounts

M

RISKS

The following accounts have never been used.
Unused accounts represent a security risk, particularly if a default password has been assigned to them, pending a change by the legitimate user.
Someone else may gain access before the real user if the initial password assigned to the account is a standard format (e.g. user's surname).

ACTIONS

Determine whether they are new accounts or the users have just never signed on to them.

M

RESULTS

```
Users with unused accounts:

CXL_SYSTEM          GENERAL SYSTEM X     | DEFAULT             GGM DEFAULT
GEN_PM              DEP - P.SMITH        | GEN_SYSTEM          GENERAL SYSTEM
GGM_TRAIN1          TRAINING 1           | XGM_DEFAULT         XGM DEFAULT BT
XGM_TRAIN1          TRAINING 1X          | YGEN_PM             DEP - P.SMITH
ZEN_PM              DEP - P.SMITH        | ZZN_PM              DEP - P.SMITH

10 users.
```

3.2 NOOWN - No owners

L

RISKS

A user has not been defined for these accounts.
Any actions performed by these accounts may not be able to be traced back to a particular person.

ACTIONS

Every account should have an owner, someone who is responsible for the actions of whoever signs on with that user-ID. When a problem arises then hopefully the System Manager will be able to question the user. Often, it is not possible to identify a specific terminal or a user-ID and so a name is vital. Some companies also include in this field the telephone extension of the user or their payroll number. These help in both locating a user quickly and identifying a user explicitly.

RESULTS

```
The following accounts do not have owners.

CXL_AFT              | CXL_AGS              | CXL_AJL
CXL_BGL              | CXL_JMJC             | CXL_JNM
CXL_JPJ              | CXL_PJM              | CXL_PRN
CXL_PS               | CXL_RH               | GEN_PJM
12 users.
```

4 SPAC - Specific accounts

RISKS

In this section we review in detail the accounts of certain standard 'system' users which appear on all similar systems.
These include SYSTEM, FIELD and DEFAULT. Each has a purpose and can also be copied to make other accounts with different names but similar properties.
Every hacker knows that these accounts exist and also that some of them are the most powerful on the system. For that reason we have chosen to pay particular attention to them in this section.
Any hacker using a terminal can enter a user name of SYSTEM or FIELD and be almost certain that there is an account on the system with that name. They then only have to determine the password which should be a difficult job.
However, if these accounts are DISUSERED then even with the correct password he could not enter the system.
Full details are given for each account followed by a list of identified problems.
If these accounts are not shown in the following pages, they were not found in your SYSUAF file and this is unusual and needs investigating.

4.1 AC-SYSTEM - SYSTEM Account

H

RISKS

This is the main Systems Manager account. His own account can be used to re-establish it when needed.
Actions carried out by the SYSMAN account could have been performed by every person who knows the password.

ACTIONS

The system manager should produce his own NAMED account which is used for day-to-day work and reserve this account for special occasions.Most managers can work perfectly well with an account which has SYSPRV and they should disuser this account.

L

RESULTS

```
System   SYSTEM MANAGER

UIC:1,4
Password length: 8                  Password lifetime: Never expires
Password last changed: 62 days.
Account expiry: None
Last interactive login: 62 days.    Last non-interactive login: 60 days.
Connections: None.

Privileges:
 Mount Netmbx Tmpmbx Group Grpprv Acnt Allspool Exquota Grpnam Prmceb
 Prmmbx Shmem Altpri Oper Pswapm Security Syslck World Diagnose Volpro
 Bypass Cmexec Cmkrnl Detach Log_IO Pfnmap Phy_IO Readall Setprv Share
 Sysnam Sysprv

Flags:
 Dispwddic
```

4.2 AC-FIELD - FIELD Account

(H)

RISKS

The FIELD account is used by service engineers when they call to do routine maintenance or in an emergency.
Since most systems have this account a hacker will try to guess this password and if they succeed, will have full control of your system. If it is DISUSERED then even guessing the password will not permit access. Try to ensure that the password has not been left as FIELD.

ACTIONS

This account should be left as DISUSERed until the engineer calls.

(L)

RESULTS

```
Field   FIELD

UIC:100,0
Password length: 6                  Password lifetime: 30 days.
Password last changed: 48 days.
Account expiry: 7 days.
Last interactive login: Never       Last non-interactive login: 43 days.
Connections: None.

Privileges:
 Netmbx Tmpmbx Group Grpnam Prmceb Prmmbx Altpri Oper Security World Volpro
 Bypass Cmkrnl Log_IO Phy_IO Readall Setprv Sysnam Sysprv

Flags:
 Dispwddic
```

4.3 AC-DEFAULT - DEFAULT Account

(H)

RISKS

This account is often used as a template to create new users from. Instead of having to define all the settings for a user, this account is used as a basis and then copied and modified slightly to create a new user account.
The privileges on this account could be increased thus affecting all users subsequently created.

ACTIONS

This account should be set up to have the minimum privileges available to a normal user (probably just TMPMBX).

(L)

RESULTS

```
Default   GGM DEFAULT

UIC:100,30
Password length: 0                  Password lifetime: Never expires
Password last changed:Pre-expired
Account expiry: None
Last interactive login: Never       Last non-interactive login: Never
Connections: None.

Privileges:
 Netmbx Tmpmbx Group Grpnam

Flags:
 Captive Dismail Restricted Dispwddic Disctly
```

5 LOGINS - Logins

RISKS

This section details how users connect to the system.

5.1 LINOI - Non-interactive Logins

L

RISKS

NON-INTERACTIVE Logins require no input from the user during the login, even though LOGINOUT still runs. These logins can be made by typing the SPAWN command or by using DECNET between network nodes.
A SUBPROCESS login occurs when a user types the DCL command RUN with any qualifiers other than /DEBUG, /DETACH or /UIC, the DCL command SPAWN, or runs a program which contains either the system routine LIB$SPAWN or $CREPRC. A SUBPROCESS login is always non-interactive.

ACTIONS

Most normal application users will not need to login non-interactively. Examines the users shown below and decide if they have appropriate access to the system.

L

RESULTS

```
The following users have logged in non-interactively:

CXL_PM                | FIELD
2 users.
```

5.2 LIBOT - Both types of login

L

RISKS

Users generally login either interactively or non-interactively. It is usually only IT staff who use both methods.

ACTIONS

We would suggest that you review the users shown below and ensure that they are all legitimate IT users.

L

RESULTS

```
The following users have logged in interactively AND non-interactively:

CXL_JMJC              | CXL_MC                | CXL_RT
GEN_MC                | SYSTEM
5 users.
```

5.3 LIINT - Interactive logins

L

RISKS

With INTERACTIVE Logins there is some communication between the program LOGINOUT.EXE and the user. The user provides LOGINOUT with responses to the 'Username' and 'Password' prompts, and, depending on the answers received, LOGINOUT will either grant or deny access to VMS.

ACTIONS

This is not a high-risk issue and most users will have interactive logins. It is shown here for completeness.

L

RESULTS

```
Of the 62 users, 44 have logged in interactively (ie from a terminal).
This is perfectly normal but we would suggest that you review the
non-interactive users too.
```

5.4 LLOGINS - Last logins

L

RISKS

Shown below are when users last logged in by any means. If the system is actively in use then most should have done so in the last 30 days. Those accounts which have not logged in for several months may no longer be needed and should be deleted by first issuing a written warning to the user.
Lots of unused accounts may indicate that when users are leaving or moving jobs, no one is informing the IT department or User Administration department.
Users who have left the company could still gain unauthorised access.

ACTIONS

A 'leavers procedure' should be established and anyone leaving the company should have their account deleted IMMEDIATELY.Review any accounts older than 60 days.

M

RESULTS

You consider 'old' accounts to be those which have not been used for more than 90 days for ordinary users and 50 days for 'system' users.
This review showed that there were 0 such accounts.

We suggest that you consider designating 'old' accounts to be those which have not been used for more than 60 days.

Distribution of last logins.

Users who have never logged in.

Last login between 151 and 300 days.

CXL_JPC	J.P.CROMPTON	255

Last login between 61 and 90 days.

CXL_AGS		64
CXL_BG	DEP - B.GOLDS	70
CXL_BPB	B.P.BROWN	64
CXL_JC	IBM - J.COOPER	63
CXL_MC	DEP - M.COOL	68
CXL_MNH	M.N.HUNTER	70
GEN_MC	DEP - M.COLLINS	68

Last login between 31 and 60 days.

CXL_AFT		43
CXL_AJL		53
CXL_BGL		46
CXL_JHM	J.H.MARTIN	43
CXL_JLP	J. PETERS	43
CXL_JMH	J. HOWELL	43
CXL_JMI	J. IVY	46
CXL_JMJC		43
CXL_JML	J. LEADBETTER	56
CXL_JMM	J. MOLESON	43
CXL_JMN	J. NORTON	46
CXL_JMS	J. SMITH	43
CXL_JNM		48
CXL_JO	J.OXSHOT	43
CXL_JPJ		46
CXL_JPL	J. LENT	43
CXL_JRD	J. ROVER	43
CXL_JS	J.SMILEY	46
CXL_JTH	J. HARRY	50
CXL_MDM	M.D.MANTA	43
CXL_MEZ	M.E.ZENT	43
CXL_MJC	M.J.COLLINS	43
CXL_MKB	M.K.BROWN	43
CXL_MLW	M.WEBSTER	43
CXL_NH	N.HOWELL	43
CXL_NJM	N.J.MILTON	43
CXL_PAC	P.A.CHIN	47
CXL_PJM		43
CXL_PJR	FX2 - P.J.ROYCE	43
CXL_PM	FX1 - P.MOON	43
CXL_PRN		43
CXL_PRT	TNT_OPER2	43
CXL_PS		43
CXL_PT	P.TELLY	43
CXL_RET	R.TAYLOR	43
CXL_RH		43
CXL_RT	R.TULL	43
FIELD	FIELD	43
GEN_PJM		43
SYSTEM	SYSTEM MANAGER	60

5.5 LIFAIL - Login failures

L

RISKS

A high number of login failure attempts indicates that:

- o you have a forgetful user
- o a process is trying to connect unsuccessfully
- o the account is under attack from someone guessing passwords

ACTIONS

You may care to discuss a sample of these with the users concerned.A very high number of failures may indicate a failing program or batch job.Remember, an account with NO login failures may mean a hacker has succeeded.

H

RESULTS

The following users have had login failures:

User-ID	Owner	Fails	Last used
CXL_AGS		12	64
CXL_BPB	B.P.BROWN	3	64
CXL_JMH	J. HOWELL	126	43
CXL_JMJC		30	43
CXL_MC	DEP - M.COOL	9	68
CXL_PJM		100	43
CXL_RT	R.TULL	6	43
CXL_SYSTEM	GENERAL SYSTEM X	20	Never
GEN_MC	DEP - M.COLLINS	9	68
GEN_PJM		100	43
GEN_PM	DEP - P.SMITH	17	Never
GEN_SYSTEM	GENERAL SYSTEM	20	Never
YGEN_PM	DEP - P.SMITH	22	Never
ZEN_PM	DEP - P.SMITH	22	Never
ZZN_PM	DEP - P.SMITH	22	Never

5.6 DEFDIR - Default Directories

L

RISKS

Default directories are the initial storage areas assigned to users.
Where people share directories they will also share data and the idea of accountability is destroyed.

ACTIONS

Ensure that users do not share default directories.

L

RESULTS

```
The following users do no have a default directory set:
CXL_JHM               J.H.MARTIN
CXL_JMJC
CXL_MC                DEP - M.COOL
CXL_PJR               FX2 - P.J.ROYCE
GEN_MC                DEP - M.COLLINS

 5 users.
```

5.7 CLI - CLI

L

RISKS

The Command Line Interpreter (CLI) is used to enter commands directly to the system. It is a standard product but others can be specified.
This is a standard product which is well known and any other CLI may behave in an unpredictable manner. It may even have malicious purposes.

ACTIONS

The CLI specified in user records should be the standard one supplied with the system.

M

RESULTS

41 accounts use the standard CLI called DCL and 21 accounts do not.

CLI = DCL2 CXL_AJL	
CLI = DCL2 CXL_JLP	J. PETERS
CLI = No CLI CXL_JMH	J. HOWELL
CLI = No CLI CXL_JO	J.OXSHOT
CLI = No CLI CXL_JPJ	
CLI = DCLX CXL_MC	DEP - M.COOL
CLI = DCL2 CXL_MJC	M.J.COLLINS
CLI = DCL2 CXL_MKB	M.K.BROWN
CLI = DCL2 CXL_MNH	M.N.HUNTER
CLI = DCL2 CXL_NH	N.HOWELL
CLI = DCL2 CXL_NJM	N.J.MILTON
CLI = DCLY CXL_PJM	
CLI = No CLI DEFAULT	GGM DEFAULT
CLI = DCLX GEN_MC	DEP - M.COLLINS
CLI = DCLY GEN_PJM	
CLI = DCL2 GGM_TRAIN1	TRAINING 1
CLI = No CLI XGM_DEFAULT	XGM DEFAULT BT
CLI = DCL2 XGM_TRAIN1	TRAINING 1X
CLI = DCL3 YGEN_PM	DEP - P.SMITH
CLI = DCL3 ZEN_PM	DEP - P.SMITH
CLI = DCL3 ZZN_PM	DEP - P.SMITH

5.8 LGICMD - LGICMD

L

RISKS

LGICMD is the name of a special file which is executed whenever a user gains access to the system.
A malicious user with access to another user's User File Directory (UFD) could copy another LOGIN.COM which contained a time-bomb or Trojan horse.

ACTIONS

It is best if these files are not called LOGIN or LOGIN.COM. A user without a LGICMD file is in a similar position.

H

RESULTS

```
The following users have bad LGICMDs:


CXL_AGS                                 LOGIN.COM
CXL_BGL                                 No LGICMD
CXL_JC                IBM - J.COOPER    No LGICMD
CXL_JNM                                 No LGICMD
CXL_JPC               J.P.CROMPTON      No LGICMD
CXL_JS                J.SMILEY          No LGICMD
CXL_MC                DEP - M.COOL      LOGIN
FIELD                 FIELD             No LGICMD
GEN_MC                DEP - M.COLLINS   LOGIN
GGM_TRAIN1            TRAINING 1        No LGICMD
SYSTEM                SYSTEM MANAGER    LOGIN
XGM_TRAIN1            TRAINING 1X       No LGICMD
```

5.9 NCAPTIVE - Non-Captive

M

RISKS

An account which is CAPTIVE cannot gain access to the operating system and so cannot use DCL commands directly.
Access to the command line could let a user do serious damage to the system.

ACTIONS

Most users should be CAPTIVE and you ought to investigate those listed below. They may be system accounts or development staff but you should satisfy yourself that each one HAS to be non-CAPTIVE.A CAPTIVE user will normally run an application program and then will be logged out when they are finished. Even when a user is CAPTIVE them may still modify files using an application such as a WP or spreadsheet so make sure you know which applications CAPTIVE users can run.

M

RESULTS

Accounts which are not captive:

CXL_AJL		CXL_BPB	B.P.BROWN
CXL_MC	DEP - M.COOL	CXL_PJM	
CXL_SYSTEM	GENERAL SYSTEM X	FIELD	FIELD
GEN_MC	DEP - M.COLLINS	GEN_PJM	
GEN_SYSTEM	GENERAL SYSTEM	SYSTEM	SYSTEM MANAGER

6 UICS - UICs

RISKS

User Identification Codes (UICs) determine a users rights on the system.

6.1 SHUICS - Shared UICs

M

RISKS

These accounts share User Identification Codes (UICs).
Users who have a common UIC will have access to each others data and the file protection scheme may not work as intended.

ACTIONS

Ensure that all users have unique UICs.

M

RESULTS

```
 The same UICs are shared by the following users:

UIC 100,10:-
  CXL_AFT             CXL_AJL             CXL_BG              CXL_BGL
   CXL_BPB             CXL_JC              CXL_JHM             CXL_JLP
   CXL_JMH             CXL_JMI             CXL_JML             CXL_JMM
   CXL_JMS             CXL_JNM             CXL_JO              CXL_JPC
   CXL_JRD             CXL_JS              CXL_JTH             GEN_PM
   YGEN_PM             ZEN_PM              ZZN_PM

UIC ?,?:-
  CXL_AGS             CXL_JMN

UIC 7,10:-
  CXL_JMJC            CXL_MC

UIC 1,10:-
  CXL_JPJ             CXL_NJM

UIC 2,10:-
  CXL_JPL             CXL_PRN             CXL_RT              GEN_MC

UIC 200,10:-
  CXL_MDM             CXL_MEZ             CXL_MJC             CXL_MKB
   CXL_MLW             CXL_MNH             CXL_NH              CXL_PAC
   CXL_PJR             CXL_PM              CXL_PRT             CXL_PS
   CXL_PT              CXL_RET             CXL_RH

UIC 5,0:-
  CXL_PJM             GEN_PJM

UIC 100,30:-
  DEFAULT             GGM_TRAIN1          XGM_DEFAULT         XGM_TRAIN1
```

6.2 LOWUICS - Low value UICs

(M)

RISKS

These accounts all have low group numbers in their UIC. The UIC is in the format [group,member]. Usually, group numbers of 10 (octal) and less fall into the category of SYSTEM and effectively are the same as users with SYSPRV. These users thus have the potential to completely control the system. Only operators and system managers should have these UICs.

ACTIONS

Examine users with low UICs and ensure that these are appropriate.

(H)

RESULTS

```
The following users have system UICs:

CXL_JMJC                                [7,10]
CXL_JPJ                                 [1,10]
CXL_JPL         J. LENT                 [2,10]
CXL_MC          DEP - M.COOL            [7,10]
CXL_NJM         N.J.MILTON              [1,10]
CXL_PJM                                 [5,0]
CXL_PRN                                 [2,10]
CXL_RT          R.TULL                  [2,10]
CXL_SYSTEM      GENERAL SYSTEM X        [3,0]
GEN_MC          DEP - M.COLLINS         [2,10]
GEN_PJM                                 [5,0]
GEN_SYSTEM      GENERAL SYSTEM          [7,0]
SYSTEM          SYSTEM MANAGER          [1,4]
 13 users have system UICs.
```

7 SYSSET - System settings

RISKS

This section looks at system settings.

7.1 UNLCPU - Unlimited cpu

M

RISKS

These users do not have their CPU time restricted.
A user performing an unusual task can 'grab' most of the CPU time and make the performance of the system become unusable for everyone else.

ACTIONS

Every user should have some form of CPU limit set. This is often felt to be difficult to do by System Managers but with careful monitoring of the systems, a reasonable limit can be established.A good starting point might be 10 hours and work down from there.

L

RESULTS

```
No users have unlimited CPU usage.
```

7.2 PRCLM - PRCLM

L

RISKS

This is the AUTHORIZE qualifier /PRCLM sub process limit. Users can spawn programs from a restricted account.

ACTIONS

This should be set to 0 to prevent a user from spawning out of a restricted account.Also ensure that the SYSGEN parameter, PQL_MPRCLM the minimum sub process limit, is set to 0.

L

RESULTS

```
The following users do not have PRCLM set to zero.

ALL users have a PRCLM limit set to zero.
```

7.3 MXDETACH - Max Detached

M

RISKS

A DETACHED login occurs when a user enters either the DCL command:

$ RUN/DETACH or $ RUN/UIC=.....

This creates a separate job running on the system. These jobs can have their own quotas and limits without sharing other resources like CPU time and can continue to exist after the original process has stopped.

ACTIONS

Unless a user has a very good reason to create a detached process it is important to limit them by NOT allowing them to create detached processes unless they have a very good reason for doing so.Users should therefore have a MAXDETACH limit of 'None'.This is not the same as 0. A MAXDETACH value of 0 (zero) permits UNLIMITED detached processes to be created which could totally disrupt your system. No privilege is required to create detached processes under a user's own UIC, but with DETACH privilege a user is allowed to create processes under ANY UIC (including System UICs).You may find that some programs will not run without a MAXDETACH of zero. This is due to lazy programming and should be discussed appropriately.

RESULTS

```
The following users have a MAXIMUM DETACHED limit NOT set to NONE.

More than 94% of users (58) have a MAXIMUM DETACHED limit NOT set to NONE.
```

8 FLAGS - Flags

RISKS

Flags are used to set a variety of user facilities. They can be turned on or off either by the system manager or the system itself.

8.1 CAPTIVE - Captive

L

RISKS

A CAPTIVE account limits the activities of the users and denies the user access to the DCL command level. Any attempt to get to DCL will result in the user being logged out (e.g. pressing Control-Y). The user cannot specify any account qualifiers when logging in such as /NOCOMMAND or /DISK.
Test accounts which are not set to CAPTIVE with the following:
Ask the user to logon as normal but with their user name, add /NOCOMMAND

Username: MyUserID/NOCOMMAND
Password: --------

The user may then get to VMS and be able to look around, delete files etc.

ACTIONS

We STRONGLY recommend that this flag is used on every user account possible and certainly on any account where a user simply runs an application and is then logged out (i.e. most normal users).

L

RESULTS

```
More than 84% of all users (52) have this flag set.
```

8.2 DISWELCOME - Diswelcome

M

RISKS

This will disable the display of the welcome message as a user logs onto the system.

ACTIONS

Do not use this flag on most users.

L

RESULTS

```
No accounts have this flag set.
```

8.3 DISNEWMAIL - Disnewmail

L

RISKS

This flag prevents users receiving notification that they have received new mail since the last time they logged in. We do not believe that this has any security significance.

ACTIONS

House-keeping only

L

RESULTS

```
No accounts have this flag set.
```

8.4 DISMAIL - Flag - Dismail

L

RISKS

This will prevent a user from using the VMS MAIL facility. If MAIL is not required, then disable it with this flag. Mail can be used to send programs to other users which may have undesirable consequences.

ACTIONS

Dismail should be applied to all users who do NOT require mail.Use this flag on most users.

H

RESULTS

```
CXL_MC          | DEFAULT          | GEN_MC           | XGM_DEFAULT
 6% of all users (4) have this flag set.
```

8.5 GENPWD - Flag - Genpwd

M

RISKS

The automatic password generator is used on these accounts. This creates random passwords which are hard to remember and experience has shown that users tend to write these down more than passwords they freely select.

ACTIONS

Use this facility only in the most secure environments.Do not use this flag on most users.

L

RESULTS

```
No accounts have this flag set.
```

8.6 DISIMAGE - Flag - Disimage

L

RISKS

The DISIMAGE flag prevents users using the MCR or RUN commands to execute system or user-written images.
Since DISIMAGE is enforced by DCL you must ensure that the account only has access to the DCL CLI.
Use this with the DEFCLI command or within a restricted account.

ACTIONS

Use this flag on most users.

H

RESULTS

```
No accounts have this flag set.
```

8.7 DISRECONNECT - Flag - Disreconnect

L

RISKS

Virtual terminals allow users to maintain more than one disconnected process at a time.

ACTIONS

Restrict the use of virtual terminals and this can be done at the user level with this flag.Use this flag on most users.

H

RESULTS

```
No accounts have this flag set.
```

8.8 DISREPORT - Flag - Disreport

H

RISKS

Setting this flag disables reporting of information concerning last logins and the number of login failures.

ACTIONS

Do not use this flag on most users.

L

RESULTS

```
No accounts have this flag set.
```

8.9 DISUSER - Flag - Disuser

L

RISKS

Accounts which are DISUSERed cannot be logged into and are effectively disabled until this flag is reset.
Seldom used accounts should be DISUSERed such as FIELD or SYSTEST.

ACTIONS

Examine the accounts below and see if they can now be disabled.Do not use this flag on most users.

L

RESULTS

```
CXL_MC           | CXL_SYSTEM       | GEN_MC           | GEN_SYSTEM
GGM_TRAIN1       | XGM_TRAIN1
 10% of all users (6) have this flag set.
```

8.10 LOCKPWD - Flag - Lockpwd

M

RISKS

This flag makes the changing of passwords only possible by the system administrator.

ACTIONS

Investigate users who have this set.Do not use this flag on most users.

L

RESULTS

```
CXL_MC           | CXL_SYSTEM       | GEN_MC           | GEN_SYSTEM
 6% of all users (4) have this flag set.
```

8.11 PWD_EXPIRED - Flag - Pwd_expired

L

RISKS

The user with this flag set has an expired password and the user has failed on their last chance to change the password.
These accounts are disabled for logins.

ACTIONS

Decide if the accounts are still needed.Do not use this flag on most users.

L

RESULTS

No accounts have this flag set.

8.12 RESTRICTED - Flag - Restricted

L

RISKS

Certain accounts require a less restricted environment than CAPTIVE accounts. Accounts used for network objects require temporary access to DCL.
Such accounts must be set up as RESTRICTED and not CAPTIVE.
RESTRICTED accounts allow the user access to DCL following the execution of the system and process login command procedures.

ACTIONS

Use this flag on most users.

L

RESULTS

More than 76% of all users (47) have this flag set.

8.13 DISPWDDIC - Flag - Dispwddic

M

RISKS

This facility disables the password dictionary facility which checks to see if a users password is in a list of standard (and easy to guess) words.

ACTIONS

Try not to use this flag - the password dictionary is a useful facility.Add variations of your company name to the dictionary as well as the local sports team's name and the words PASSWORD and SECRET.Use this flag on most users.

H

RESULTS

More than 98% of all users (61) have this flag set.

8.14 DEFCLI - Flag - Defcli

M

RISKS

This flag prevents a user using another CLI, other than DCL when logging in.

ACTIONS

Use this flag on most users.

H

RESULTS

```
No accounts have this flag set.
```

8.15 DISCTLY - Flag - Disctly

L

RISKS

This is designed to prevent users pressing Control-Y keys and dropping out of the application to DCL.

ACTIONS

Use this on all accounts which are not marked as captive and do not need access to VMS.Use this flag on most users.

L

RESULTS

```
More than 77% of all users (48) have this flag set.
```

8.16 AUDIT - Flag - Audit

L

RISKS

Enables or disables the security auditing of all operations of a user that can be audited.

ACTIONS

This can cause serious performance problems and should be used carefully.Do not use this flag on most users.

L

RESULTS

```
CXL_AFT          | CXL_MLW
 3% of all users (2) have this flag set.
```

8.17 AUTOLOGIN - Flag - AutoLogin

L

RISKS

This flag restricts the user to using the autologin mechanism to log in to an account.
When this is set the user cannot login at any terminal that requires user-ID and password.

ACTIONS

Do not use this flag on most users.

L

RESULTS

```
No accounts have this flag set.
```

8.18 DISFORCE_PWD_CHANGE - Flag - Disforce_pwd_change

M

RISKS

This removes the need for a user to change an expired password when they login.
We would not recommend the use of this flag.

ACTIONS

Do not use this flag on most users.

L

RESULTS

```
No accounts have this flag set.
```

8.19 DISPWDHIS - Flag - Dispwdhis

M

RISKS

This flag disables the checking of user's passwords against a history file of their old ones.
Check user's password history is a useful security facility which should be applied whenever possible.
It is designed to prevent a user flipping between just two passwords.

ACTIONS

Do not use this flag on most users.

L

RESULTS

```
No accounts have this flag set.
```

8.20 PWD2_EXPIRED - Flag - Pwd2_Expired

L

RISKS

This flag, when set, will mark the secondary password as expired and thus force the user to change it when they log in.

ACTIONS

It may be excessive in many businesses to have a secondary password.Do not use this flag on most users.

RESULTS

```
CXL_AFT          | CXL_NJM
 5% of all users (3) have this flag set.
```

8.21 EXTAUTH - Flag - External authentication

RISKS

External authentication allows users to log in at the OpenVMS login prompt using their external user IDs and passwords. The system considers users to be authenticated by their external user name and password, not by the SYSUAF user name and password.
The system still uses the SYSUAF record to check a user's login restrictions and quotas and to create the user's process profile.
For example, a user may be authenticated under Windows NT and then be allowed on to the system. PATHWORKS and Advanced Server for OpenVMS authentication modules are supported as external authenticators, providing NT-compatible authentication of OpenVMS users.

ACTIONS

Use this flag only where necessary.

RESULTS

```
No accounts have this flag set.
```

8.22 VMSAUTH - Flag - VMSauth

RISKS

Allows account to use standard (SYSUAF) authentication when the EXTAUTH flag would otherwise require external authentication. This depends on the application. An application specifies the VMS domain of interpretation when calling SYS$ACM to request standard VMS authentication for a user account that normally uses external authentication

ACTIONS

Use this flag only where necessary.

RESULTS

```
No accounts have this flag set.
```

8.23 PWDMIX - Flag - PwdMix

M

RISKS

Enables case-sensitive and extended-character passwords.
After PWDMIX is specified, you can use mixed-case and extended characters in passwords.
Be aware that before the PWDMIX flag is enabled, the system stores passwords in all upper-case. Therefore, until you change passwords, you must enter your pre-PWDMIX passwords in upper-case.

ACTIONS

All users should have this flag set.

L

RESULTS

```
CXL_JO          | ZZN_PM
 3% of all users (2) have this flag set.
```

8.24 DISPWDSYNCH - Flag - DisPwdSynch

L

RISKS

Suppresses synchronization of the external password for this account.

ACTIONS

Set as necessary.

L

RESULTS

```
CXL_JHM         | CXL_MLW         | ZEN_PM
 5% of all users (3) have this flag set.
```

9 LEVELS - Levels

RISKS

The privileges assigned to users have been graded by HP into 7 levels
(0 to 6) as follows:
0 None - No privileges.
1 Normal - Minimum privileges to effectively use the system.
2 Group - Potential to interfere with members of the same group.
3 Devour - Potential to consume non-critical system wide resources.
4 System - Potential to interfere with normal system operation.
5 Files - Potential to compromise file security.
6 All - Potential to control the system.
This grading is based on the potential damage that the user can cause to the system.
Each privilege has been divided as follows:
0 None None
1 Normal MOUNT NETMBX TMPMBX
2 Group GROUP GRPPRV
3 Devour ACNT ALLSPOOL BUGCHK EXQUOTA GRPNAM PRMCEB PRMGBL PRMMBX SHMEM
4 System ALTPRI OPER PSWAPM WORLD SECURITY SYSLCK
5 Files DIAGNOSE SYSGBL VOLPRO
6 All BYPASS CMEXEC CMKRNL DETACH LOG_IO PFNMAP PHY_IO
READALL SETPRV SHARE SYSNAM SYSPRV IMPERSONATE
The most damaging privileges are those, at or above level 4. It should be borne in mind that anyone who can modify the privileges through the use of the AUTHORIZE program can give themselves privileges of the highest level. They can also create users with these privileges and access these accounts whenever they like.
If the person granting these privileges does not know 100% what a privilege does, it should not be granted to any user.
Most users should be at or below level 3 and generally only level 1 privileges are needed to run most normal applications.
Query all level 4 to 6 users. They all have high level access to your system.

9.1 LEVELS4-6 - Levels 4 to 6

H

RISKS

The privileges assigned to users have been graded by HP into 7 levels. The most critical are levels 4 to 6.

ACTIONS

Examine each user at their associated level and ensure that they have the correct level for their job.Ensure that ordinary application users are in levels 0 to 2 (ie not show in the list below)Ensure computer operators are at levels 0 to 4

H

RESULTS

```
Users with level 4 accounts.
----------------------------
CXL_AJL         | CXL_PRN         | CXL_PRT         | CXL_SYSTEM

There are 4  users at this level.

Users with level 5 accounts.
----------------------------

No users at this level.

Users with level 6 accounts.
----------------------------
CXL_BPB         | CXL_JML         | CXL_MC          | CXL_MKB
CXL_PJM         | FIELD           | GEN_MC          | GEN_PJM
GEN_SYSTEM      | SYSTEM

There are 10  users at this level.
```

10 PRIVS - Privileges

RISKS

Privileges restrict the use of certain system functions to processes created on behalf of authorized users.
Some system activities are limited by a users' privileges. These are used to ensure the integrity of the system and the data it holds. Privileges should only be granted to users for two reasons:
o The user actually needs it.
o The user has the skill to use it without disrupting the system.
A user's privileges are recorded in their user record and show both the authorised and the default privileges.
Some users might need a particular program to run with certain privileges. This can be achieved WITHOUT giving the privilege to the user by using the VMS Install Utility to give the privilege to the program and then putting an ACL on the executable image.
Users would effectively possess the privilege only when they are actually executing the image. (Note - All images installed with privilege must be linked with the /NOTRACEBACK qualifier to prevent on-line bugging and traceback.)

10.1 ACNT - Privilege - Acnt

L

RISKS

A user who has ACNT privilege can create sub processes or detached processes in which accounting is disabled. Thus, only such a privileged user can enter the DCL command RUN with the /NOACCOUNTING qualifier or inhibit accounting in the Create Process ($CREPRC) system service.

ACTIONS

Do not give this privilege to most users.

L

RESULTS

```
SYSTEM

  2% of users (1) have this privilege.
```

10.2 ALLSPOOL - Privilege - Allspool

L

RISKS

The ALLSPOOL privilege allows the user to allocate a spooled device by executing the Allocate Device ($ALLOC) system service or by using the DCL command ALLOCATE.

ACTIONS

This privilege should only be granted to users who need to perform logical or physical I/O operations to a spooled device.Do not give this privilege to most users.

L

RESULTS

```
SYSTEM

  2% of users (1) have this privilege.
```

10.3 ALTPRI - Privilege - Altpri

M

RISKS

The ALTPRI privilege allows a user to:

- Increase their own base priority.
- Set the base priority of another process to a value higher than that of the target process.

ACTIONS

This privilege should not be granted widely. If unqualified users have the unrestricted ability to set base priorities, fair and orderly scheduling of processes for execution can easily be disrupted.Do not give this privilege to most users.

L

RESULTS

```
FIELD            | SYSTEM

  3% of users (2) have this privilege.
```

10.4 BUGCHK - Privilege - BugChk

M

RISKS

The use of BUGCHK privilege should be restricted to supplied system software that uses the VMS Bugcheck Facility. The privilege allows the user to make bugcheck error log entries.

ACTIONS

Do not give this privilege to most users.

L

RESULTS

```
No users have this privilege.
```

10.5 BYPASS - Privilege - ByPass

M

RISKS

The BYPASS privilege allows a user to have read, write, execute and delete access to all files, bypassing any restrictions, either UIC or ACL based.

ACTIONS

Grant this with extreme caution, as it overrides all file protection. It should be reserved for use by either well-tested, reliable programs and command procedures or system backup operation. SYSPRV is acceptable for interactive use, as it ultimately grants access to all files while still providing access checks.Do not give this privilege to most users.

H

RESULTS

```
CXL_MKB          | CXL_PJM          | FIELD            | GEN_PJM
SYSTEM

  8% of users (5) have this privilege.
```

10.6 CMEXEC - Privilege - Cmexec

L

RISKS

The CMEXEC privilege allows the user to execute the Change Mode to Executive ($CMEXEC) system service.
Grant this privilege only to users who need to gain access to protected and sensitive data structures and internal functions of the operating system.

ACTIONS

If unqualified users have unrestricted access to sensitive data structures and functions, the operating system and service to other users can be easily disrupted. Such disruptions can include failure of the system, destruction of the database and exposure of confidential information.Do not give this privilege to most users.

L

RESULTS

```
SYSTEM

  2% of users (1) have this privilege.
```

10.7 CMKRNL - Privilege - Cmkrnl

M

RISKS

The CMKRNL privilege allows the user to execute the Change Mode to Kernel ($CMKRNL) system service.

ACTIONS

This should only be granted to users who need to execute privileged instructions or who need to gain access to the most protected or sensitive data structures and functions of the operating system.Unqualified use can result in disruption of the operating system, destruction of the database and exposure of confidential information.Subjects holding CMKRNL can use the DCL command $ SET UIC [3,7] and thereby collect a System UIC.Do not give this privilege to most users.

M

RESULTS

```
FIELD            | SYSTEM

  3% of users (2) have this privilege.
```

10.8 DETACH - Privilege - Detach

L

RISKS

Users with DETACH privilege can create detached processes that have their own UIC without the DETACH privilege, provided the users do not exceed their MAXJOBS and MAXDETACH quotas. However, the DETACH privilege becomes valuable when a user wants to specify a different UIC for the detached process. There is no restriction on the UIC that can be specified for a detached process if you have the DETACH privilege. Thus, there are no restrictions on the files and directories to which a detached process can gain access. DETACH allows the user to crease detached processes. These processes remain in existence even after the user who has logged off the system. An example of a detached process is the process created by the system for a user when the user logs in to the system.

ACTIONS

Do not give this privilege to most users.

L

RESULTS

```
SYSTEM

  2% of users (1) have this privilege.
```

10.9 DIAGNOSE - Privilege - Diagnose

L

RISKS

The DIAGNOSE privilege allows the user to run on-line diagnostic programs and to intercept and copy all messages written to the error log file.

ACTIONS

Do not give this privilege to most users.

L

RESULTS

```
SYSTEM

 2% of users (1) have this privilege.
```

10.10 EXQUOTA - Privilege - Exquota

RISKS

The EXQUOTA privilege allows the space taken by the user's files on given disk volumes to exceed any usage quotas set for the user (as determined by the UIC) of those volumes.

ACTIONS

Do not give this privilege to most users.

RESULTS

```
SYSTEM

 2% of users (1) have this privilege.
```

10.11 GROUP - Privilege - Group

RISKS

The GROUP privilege allows the user to affect other processes in its own group by executing the following process control system services:

Suspend Process ($SUSPND) Resume Process ($RESUME)
Delete Process ($DELPRC) Set Priority ($SETPRI)
Wake ($WAKE) Schedule Wakeup ($SCHDWK)
Cancel Wakeup ($CANWAK) Force Exit ($FORCEX)

The user is also allowed to examine other processes in its own group by executing the Get Job/Process Information ($GETJPI) system service. A user process with GROUP privilege can issue the SET PROCESS command for other processes in its group.

GROUP privilege is not needed for a user to exercise control over, or to examine, sub processes that they created or other detached processes of their UIC. You should, however, grant this privilege to users who need to exercise control over the processes and operations of other members of their UIC group.

ACTIONS

Do not give this privilege to most users.

RESULTS

```
All users have this privilege.
```

10.12 GRPNAM - Privilege - Grpnam

RISKS

The GRPNAM privilege allows a user to insert and delete names to and from the logical name table of the group to which the user belongs.
In addition, the privileged user can use the DCL commands ASSIGN and DEFINE to add names to the group logical name table, the DCL command DEASSIGN to delete names from the table, and the /GROUP qualifier of the DCL command MOUNT to share volumes among group members.

ACTIONS

Do not grant this privilege to all users of the system because it allows the user to create an unlimited number of group logical names. When unqualified users have the unrestricted ability to create group logical names, excessive use of system dynamic memory can degrade system performance. In addition, a user with the GRPNAM privilege can interfere with the activities of other users in the same group by creating definitions of commonly used logical names such as SYS $SYSTEM.Do not give this privilege to most users.

RESULTS

```
All users have this privilege.
```

10.13 GRPPRV - Privilege - Grpprv

RISKS

The GRPPRV privilege allows a user access to a file using the file's SYSTEM protection field when the user's group matches the group of the file owner.
GRPPRV also allows a user to change the protection of any file whose owner group matches the user's group. This privilege also allows a user to change the ownership of objects within the user's group.

ACTIONS

Grant this privilege only to users who function as group managers. Note that if any member of a group holds any of the privileges in the 'ALL' category, then any other member of that group who holds GRPPRV privilege can gain control of the system by indirectly acquiring that privilege. A user with GRPPRV privilege, whose UIC group matches an object's owner group, will receive access in the SYSTEM category.Do not give this privilege to most users.

RESULTS

```
SYSTEM

  2% of users (1) have this privilege.
```

10.14 LOGIO - Privilege - LogIO

RISKS

The LOG_IO privilege allows the user to execute the QUEUE I/O REQUEST system service to perform logical-level I/O operations. LOG_IO privilege is also required for certain device control functions, such as setting permanent terminal characteristics.

ACTIONS

Grant this privilege only to users who need it since it allows them to access data anywhere on a volume without worrying about any file structure. If this privilege is given to users who have no need for it, the operating system and service to other users can be easily disrupted. Such disruptions can include the destruction of information on the system device, the destruction of user data, and the exposure of confidential information.Do not give this privilege to most users.

M

RESULTS

```
FIELD            | SYSTEM

  3% of users (2) have this privilege.
```

10.15 MOUNT - Privilege - Mount

M

RISKS

The MOUNT privilege allows a user to execute the mount volume QIO function.

ACTIONS

Restrict the use of this function to system software supplied by DEC.Do not give this privilege to most users.

L

RESULTS

```
SYSTEM

  2% of users (1) have this privilege.
```

10.16 NETMBX - Privilege - Netmbx

L

RISKS

The NETMBX privilege allows the user to perform functions related to a DECNET computer network. The privilege is granted to all general users who need to access the network. However, if they have NETMBX then they can MAIL and PHONE across the network, as well as doing SET HOST.

ACTIONS

Give this privilege to most users.

L

RESULTS

```
All users have this privilege.
```

10.17 OPER - Privilege - Oper

M

RISKS

The OPER privilege allows the user to use the Operator Communication Manager (OPCOM) process as follows:

- o reply to users requests
- o broadcast messages to all terminals logged in
- o designate terminals as operators terminals
- o initialise and control the log file of operators' messages
- o set spooled devices
- o control queues

ACTIONS

Grant this privilege ONLY to the operators of the system. A user with this privilege is able to obtain full access to the whole system.Do not give this privilege to most users.

M

RESULTS

```
CXL_AJL          | CXL_MC           | CXL_MKB          | CXL_PJM
CXL_PRN          | CXL_PRT          | CXL_SYSTEM       | FIELD
GEN_MC           | GEN_PJM          | GEN_SYSTEM       | SYSTEM

  19% of users (12) have this privilege.
```

10.18 PFNMAP - Privilege - Pfnmap

L

RISKS

The PFNMAP privilege allows the user to map to specific pages of physical memory or I/O device registers, no matter who is using the pages or registers.

ACTIONS

If used by unqualified users, the operating system and service to others can easily be disrupted.Do not give this privilege to most users.

L

RESULTS

```
SYSTEM

  2% of users (1) have this privilege.
```

10.19 PHYIO - Privilege - Phyio

M

RISKS

The PHY_IO privilege allows the user to execute the Queue I/O Request ($QIO) system service to perform physical-level I/O operations.

ACTIONS

Grant the PHY_IO privilege only to users who need it; this privilege should be granted even more carefully than the LOG_IO privilege. If this privilege is given to unqualified users who have no need for it, the operating system and service to other users can be easily disrupted. Such disruptions can include the destruction of information on the system device, the destruction of user data, and the exposure of confidential information.Do not give this privilege to most users.

M

RESULTS

```
FIELD            | SYSTEM

  3% of users (2) have this privilege.
```

10.20 PRMCEB - Privilege - Prmceb

L

RISKS

The PRMCEB privilege allows a user to create or delete a permanent common event flag cluster by executing the Association Common Event Flag Cluster or Delete Common Event Flag Cluster system service. Common event flag clusters enable co-operating processes to communicate with each other and thus provide the means of synchronising their execution.

ACTIONS

Do not grant this privilege to all users of the system because it allows the user to create an unlimited number of permanent common event flag clusters. A permanent cluster remains in the system even after the creating process has been terminated and continues to use up a portion of system dynamic memory. When many users have the unrestricted ability to create permanent common event flag clusters, the excessive use of system dynamic memory can degrade system performance.Do not give this privilege to most users.

L

RESULTS

```
FIELD            | SYSTEM

  3% of users (2) have this privilege.
```

10.21 PRMGBL - Privilege - Prmgbl

L

RISKS

The PRMGBL privilege allows a user to create permanent global sections by executing the Create and Map Section ($CRMPSC) system service. In addition, the user with this privilege (plus CMKRNL and SYSGBL privileges) can use the VMS Install Utility.
Global sections are shared structures that can be mapped simultaneously in the virtual address space of many processes. All processes see the same code or data. Global sections are used for re-entrant subroutines or data buffers.
If permanent global sections are not explicitly deleted, they tie up space in the global section and global page limited resources.

ACTIONS

Grant this privilege with care.Do not give this privilege to most users.

RESULTS

```
No users have this privilege.
```

10.22 PRMMBX - Privilege - Prmmbx

RISKS

The PRMMBX allows a user to create or delete a permanent mailbox by executing the Create Mailbox and Assign Channel ($CREMBX) system service of the Delete Mailbox ($DELMBX) system service. Mailboxes are buffers in virtual memory that are treated as if they were record-oriented I/O devices. A mailbox is used for general interprocess communication.
Permanent mailboxes are not automatically deleted when the creating processes are deleted and thus continue to use a portion of system dynamic memory.

ACTIONS

Do not give this privilege to most users.

RESULTS

```
FIELD           | SYSTEM

  3% of users (2) have this privilege.
```

10.23 PSWAPM - Privilege - Pswapm

RISKS

The PSWAPM privilege allows the user's process to control whether it can be swapped out of the balance set by executing the Set Process Swap Mode ($SETSWM) system service. A process must have this privilege to lock itself in the balance set (i.e. to disable swapping), or to unlock itself from the balance set (i.e. to enable swapping).
With this privilege, a process can create a process that is locked in the balance set (process swap mode disabled) by using an optional argument to the Create Process ($CREPRC) system service or, when the DCL command RUN is used to create a process, by using a qualifier of the RUN command.
Grant this privilege only to users who need to lock a process in memory for performance reasons. Typically, this will be a real-time process.

ACTIONS

Do not give this privilege to most users.

L

RESULTS

```
SYSTEM

  2% of users (1) have this privilege.
```

10.24 READALL - Privilege - Readall

H

RISKS

The READALL privilege allows the process to bypass existing restrictions that would otherwise prevent the process from reading a file. However, unlike the BYPASS privilege which permits writing a deleting, READALL only permits reading of the file and control operations (such as changing protection and writing the backup date).

ACTIONS

Grant this privilege to operators so they can perform system backups. The implications of this privilege are the same as those for the SYSPRV privilege. A user with READALL privilege receives READ and CONTROL access to an object even if that access is denied by the ACL or UIC-based protection.Do not give this privilege to most users.

H

RESULTS

```
CXL_MC          | FIELD           | GEN_MC          | SYSTEM

  6% of users (4) have this privilege.
```

10.25 PSECY - Privilege - Security

H

RISKS

SECURITY allows a user to perform security related functions such as disabling of security audits or setting the system password.

ACTIONS

Grant this privilege only to security administrators. Irresponsible users who obtain the privilege can subvert the system's security auditing and can lock out users through improper application of system passwords.Do not give this privilege to most users.

L

RESULTS

```
FIELD            | SYSTEM

 3% of users (2) have this privilege.
```

10.26 SETPRV - Privilege - Setprv

M

RISKS

The SETPRV privilege allows the user's process to create processes whose privileges are greater than its own by executing the Create Process ($CREPRC) system service with an optional argument, or by issuing the DCL command RUN to create a process. A user with this privilege can also execute the DCL command SET PROCESS/PRIVILEGES to obtain any desired privilege.

ACTIONS

Exercise the same caution in granting SETPRV as in granting any other privilege since SETPRV allows the user to enable any or all privileges.Do not give this privilege to most users.

M

RESULTS

```
FIELD            | SYSTEM

 3% of users (2) have this privilege.
```

10.27 SHARE - Privilege - Share

L

RISKS

The SHARE privilege allows users to assign channels to devices allocated to other processes.

ACTIONS

Grant this privilege only to system processes such as print symbionts. This privilege would allow an irresponsible user to interfere with the operation of devices belonging to other users.Do not give this privilege to most users.

L

RESULTS

```
SYSTEM

 2% of users (1) have this privilege.
```

10.28 SHMEM - Privilege - Shmem

L

RISKS

The SHMEM privilege allows the user's process to create global sections and mailboxes (permanent and temporary) in multiport memory if the process also has appropriate PRMGBL, PRMMBX, SYSGBL and TMPMBX privilege. Just as in local memory, the space required for a multiport memory temporary mailbox counts against the buffered I/O byte count limit (BYTLM) of the process.

ACTIONS

Do not give this privilege to most users.

L

RESULTS

```
SYSTEM

 2% of users (1) have this privilege.
```

10.29 SYSGBL - Privilege - Sysgbl

M

RISKS

The SYSGBL privilege lets a user create system global sections by executing the Create and Map Section ($CRMPSC) system service. In addition, the user with this privilege (plus the CMKRNL and PRMGBL privileges) can use the VMS Install Utility.

ACTIONS

Exercise caution in granting this privilege. System global sections require space in the global section and page tables, which are limited resources.Do not give this privilege to most users.

L

RESULTS

```
No users have this privilege.
```

10.30 SYSLCK - Privilege - Syslck

M

RISKS

The SYSLCK privilege allows a user to lock system wide resources with the Enqueue Lock Request ($ENQ) system service. Grant this privilege to users who need to run programs that lock resources in the system wide resource name space.

ACTIONS

Exercise caution in granting this privilege. Users who hold the SYSLCK privilege can interfere with the synchronisation of system software and all other user software as well.Do not give this privilege to most users.

L

RESULTS

```
SYSTEM

  2% of users (1) have this privilege.
```

10.31 SYSNAM - Privilege - Sysnam

H

RISKS

The SYSNAM privilege allows the user's process to insert and delete names in the system logical name table. This privilege also permits the creation of executive mode logical names. In addition, the user with this privilege can use the DCL commands ASSIGN and DEFINE to add names to the system logical name table, and can use the DEASSIGN command to delete names from the table.
A user with SYSNAM privilege could define such critical system logical names as SYS$SYSTEM AND SYSUAF, thus gaining control of the system.

ACTIONS

Grant this privilege only to the system operators or to system programmers who need to define system logical names (such as names for user devices, library directories, and the system directory).Do not give this privilege to most users.

M

RESULTS

```
FIELD            | SYSTEM

  3% of users (2) have this privilege.
```

10.32 SYSPRV - Privilege - Sysprv

H

RISKS

The SYSPRV privilege gives users the access rights accorded to users in the SYSTEM category regardless of the group portion of the UIC.
These users have the ability to change user privileges and even create new accounts through the AUTHORIZE program.

ACTIONS

Do not give this privilege to most users.

M

RESULTS

```
CXL_BPB          | FIELD            | SYSTEM

  5% of users (3) have this privilege.
```

10.33 TMPMBX - Privilege - Tmpmbx

L

RISKS

The TMPMBX privilege allows the user to create a temporary mailbox by executing the Create Mailbox and Assign Channel ($CREMBX) system service.
Mailboxes are buffers in memory that are treated as if they were record oriented I/O devices. A mailbox is used for interprocess communication. Grant this privilege to all users of the system to facilitate interprocess communications. System performance is no likely to be degraded by permitting the creation of temporary mailboxes, because their number is controlled by limits on the use of system dynamic memory (BYTLM quota).

ACTIONS

Give this privilege to most users.

L

RESULTS

```
All users have this privilege.
```

10.34 VOLPRO - Privilege - Volpro

L

RISKS

The VOLPRO privilege allows the user to perform the following tasks:
o initialise a previously used volume with an owner UIC different from the user's own UIC
o override the expiration date on a tape or disk volume owned by another user
o override the owner UIC protection of a volume.
The VOLPRO privilege permits control only over volumes that the user can mount or initialise. Volumes mounted with the /SYSTEM qualifier are safe from the user with the VOLPRO privilege as long as the user does not also have the SYSNAM privilege.

ACTIONS

Exercise extreme caution in granting the VOLPRO privilege. If unqualified users can override volume protection, the operating system and service to others can be disrupted. Such disruptions can include destruction of the database and exposure of confidential information.Do not give this privilege to most users.

M

RESULTS

```
FIELD            | SYSTEM

  3% of users (2) have this privilege.
```

10.35 WORLD - Privilege - World

L

RISKS

The WORLD privilege allows the user to affect other processes both inside and outside its group by executing the following process control system services:
o Suspend Process ($SUSPND) o Resume Process ($RESUME)
o Delete Process ($DELPRC) o Set Priority ($SETPRI)
o Wake ($WAKE) o Schedule Wakeup ($SCHDWK)
o Cancel Wakeup ($CANWAK) o Force Exist ($FORCEX).
The user is also allowed to examine processes outside their own group. A user with WORLD privilege can issue the SET PROCESS command for all processes.
To exercise control over or examine sub processes that they created a user needs no special privilege. To affect or examine other processes inside its own group, a process needs only the GROUP privilege. To affect or examine processes outside its own group, a process needs the WORLD privilege.

ACTIONS

Do not give this privilege to most users.

L

RESULTS

```
FIELD            | SYSTEM

  3% of users (2) have this privilege.
```

10.36 AUDIT - Privilege - Audit

M

RISKS

This privilege allows programs to add audit records to the security log file. It should only be used with a process and not a user.
It will allow the recording of events which seem to have come from the operating system or another user process.

ACTIONS

Do not give this privilege to most users.

L

RESULTS

```
GEN_PJM

  2% of users (1) have this privilege.
```

10.37 DGRADE - Privilege - Downgrade

M

RISKS

This privilege permits a process to manipulate mandatory access controls and is reserved for use by security products.

ACTIONS

No users should have this privilege.

L

RESULTS

```
No users have this privilege.
```

10.38 PIMPT - Privilege - Import

L

RISKS

This privilege lets a process change mandatory access controls and will for example let a process mount unlabeled tape volumes. It is reserved for enhanced security products.

ACTIONS

No users should have this privilege.

L

RESULTS

```
No users have this privilege.
```

10.39 UGRADE - Privilege - Upgrade

L

RISKS

This privilege permits a process to manipulate mandatory access controls and is reserved for use by security products. No users should have this privilege.

ACTIONS

No users should have this privilege.

L

RESULTS

```
No users have this privilege.
```

10.40 IPNATE - Privilege - Impersonate

M

RISKS

This privilege is a replacement for the DETACH privilege.
Users with IMPERSONATE privilege can create detached processes that have their own UIC without the IMPERSONATE privilege, provided the users do not exceed their MAXJOBS and MAXDETACH quotas. However, the IMPERSONATE privilege becomes valuable when a user wants to specify a different UIC for the detached process.
There is no restriction on the UIC that can be specified for a detached process if you have the IMPERSONATE privilege. Thus, there are no restrictions on the files and directories to which a detached process can gain access. IMPERSONATE allows the user to crease detached processes. These processes remain in existence
even after the user who has logged off the system. An example of a detached process is the process created by the system for a user when the user logs in to the system.

ACTIONS

Do not give this privilege to most users.

M

RESULTS

```
CXL_JML          | CXL_MC           | GEN_SYSTEM

  5% of users (3) have this privilege.
```

10.41 OVERALL - Flags/Privilege - Overall

M

RISKS

This section of the report is a detailed review of the users. The user and privilege level is given and then areas of possible concern are indicated.
Next to each problem is a number in brackets and this can be cross referenced to the problem numbers shown at the end of this report which explains the significance of each problem.
We also indicate where users have very high access to the system and in some instances this may be completely appropriate (e.g. SYSTEM) but all instances should be reviewed carefully.

ACTIONS

Review each user and determine which problems should be fixed immediately.

L

RESULTS

```
 Key:
 AOPSSWA                    Level4 Privileges    ALTPRI OPER PSWAPM SECURITY SYSLCK
WORLD AUDIT
 DSVI                       Level5 Privileges    DIAGNOSE SYSGBL VOLPRO IMPORT
 BCCDLPPRSSSSDUI            Level6 Privileges    BYPASS CMEXEC CMKRNL DETACH LOG_IO
PFNMAP
                                                 PHY_IO READALL SETPRV SHARE SYSNAM
SYSPRV
                                                 DOWNGRADE UPGRADE IMPERSONATE
 CDDDGDDDDLPRDDDAADDPEVPD   Flags                Captive, Diswelcome, Disnewmail,
etc.
 NBLDR                      Connections          Network, Batch, Local, Dial-up,
Remote

                |AOPSSWA|DSVI|BCCDLPPRSSSSDUI|CDDDGDDDDLPRDDDAADDPEVPD|NBLDR
 USER-ID        |LEVEL4 | L5 |     LEVEL6    |          FLAGS          | CON.
 ---------------|-------|----|---------------|-------------------------|-----
 GEN_PM         |.......|....|...............|C..........D..........|.....
 FIELD          |AO.S.W.|..V.|B.C.L.PRS.SS...|..........D..........|.....
 GEN_MC         |.O.....|....|.......R.......|...D....DL..D..........|.....
 GEN_PJM        |.O....A|....|B..............|..........D..........|.....
 GEN_SYSTEM     |.O.....|....|..............I|........DL..D..........|.....
 DEFAULT        |.......|....|...............|C..D.......RD.D.........|.....
 GGM_TRAIN1     |.......|....|...............|C.......D..RD.D.........|.....
 CXL_JC         |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_AFT        |.......|....|...............|C..........RD.DA...P....|NBL.R
 CXL_AGS        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_JPC        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_AJL        |.O.....|....|...............|.......................|N.L.R
 CXL_JLP        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_JMJC       |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_JMH        |.......|....|...............|C..........RD.D.........|NBL..
 CXL_JMI        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_JML        |.......|....|..............I|C..........RD.D.........|NBL.R
 CXL_JMM        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_JMN        |.......|....|...............|C..........RD.D.........|NBL..
 CXL_JMS        |.......|....|...............|C..........RD.D.........|.BL..
 CXL_JNM        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_JO         |.......|....|...............|C..........RD.D.......P.|NBL.R
 CXL_JPJ        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_JPL        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_JRD        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_JS         |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_JTH        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_BG         |.......|....|...............|C..........RD.D.........|..L.R
 CXL_BGL        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_JHM        |.......|....|...............|C..........RD..........D|NBL.R
 CXL_BPB        |.......|....|...........S...|..........RD.D.........|NBL.R
 CXL_MDM        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_MEZ        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_MJC        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_MKB        |.O.....|....|B..............|C..........RD.D.........|NBL.R
 CXL_MLW        |.......|....|...............|C..........RD.DA.......D|NBL.R
 CXL_MNH        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_NH         |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_NJM        |.......|....|...............|C..........RD.D....P....|NBL.R
 CXL_PAC        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_PT         |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_PJR        |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_PM         |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_PS         |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_PRN        |.O.....|....|...............|C..........D.D.........|NBL.R
 CXL_PRT        |.O.....|....|...............|C..........D.D.........|NBL.R
 CXL_RT         |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_RET        |.......|....|...............|C..........RD.D.........|NBL.R
 SYSTEM         |AOPSSW.|D.V.|BCCDLPPRSSSS...|..........D..........|.....
 CXL_RH         |.......|....|...............|C..........RD.D.........|NBL.R
 CXL_MC         |.O.....|....|.......R......I|...D....DL..D..........|.....
```