



How To Prevent Common OS/400® Security Exposures 32E

2003

iSeries and AS/400 Connection Conference

by

Wayne O. Evans



iSeries® has an excellent security implementation

- ◆ Machine instructions enforce access control
- ◆ Object architecture prevents virus
- ◆ Security controls integrated into OS/400

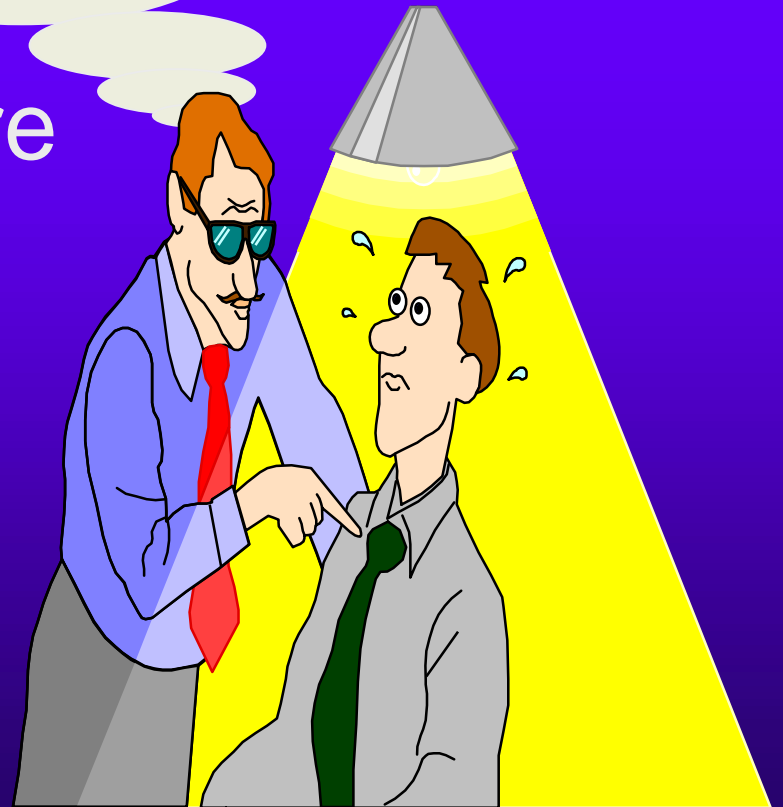
Security is designed
into OS/400

**But YOU have to
activate security**



Is your System Secure?

- ◆ You must configure security correctly
- ◆ You must avoid common security exposures



Common Security Exposures

1. Effective written security policy
2. Security Level below 40
3. Control PC and remote system access
4. Restricting Operations Navigator
5. Excessive command line access
6. Inactive user profiles
7. Excessive special authorities
8. Elimination of trivial passwords
9. Authority to user profiles
10. Object ownership and access



#1 –Security Policy

◆ Challenge

- Do you have a security policy to direct security decisions?
- Is your security policy current?
- Are users **aware and understand** your security policy?

◆ Remedy

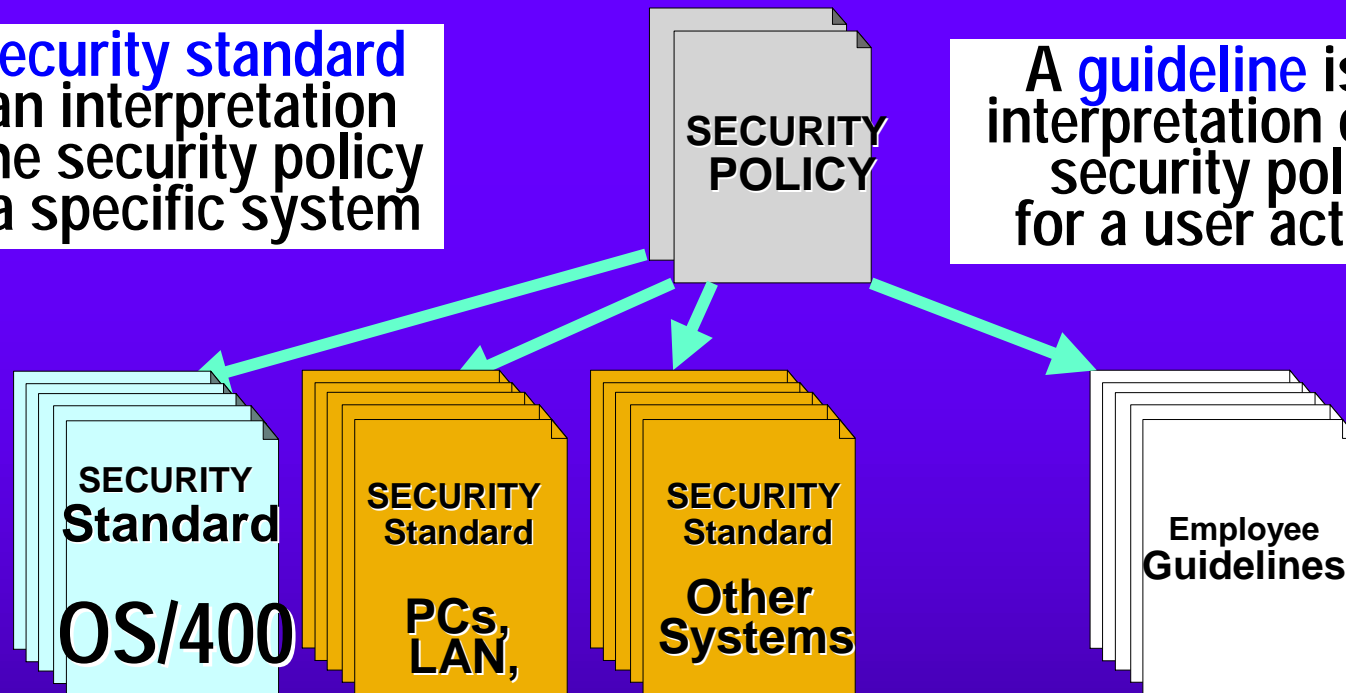
- Download sample policies from
WWW.WOEVANS.COM

Security Policy = Plan for Security

Levels of Documentation

A **security standard** is an interpretation of the security policy for a specific system

A **guideline** is an interpretation of the security policy for a user actions



1. **Policy** – High level objectives
2. **Standard** – System specific
3. **Guideline** – User instructions

#2 – System Security Level

◆ Challenge

- System value QSECURITY sets protection level
 - Level 20 menu security only (Strongly discouraged)
 - Level 30 menu and object security (Not recommended)
 - Level 40 additional integrity protection **(RECOMMENDED)**
 - Level 50 C2 level of protection (Overkill)

◆ Remedy

- Activate audit to determine if you can move to security level 40



#2 – System Security Level

1. Do not change system value QSECURITY immediately
2. Start up auditing and collect data thru a month-end close
3. Review audit log
4. If no problems are found, then move to level 40

More details download article
"Moving to Security Level 40" from
WWW.WOEVANS.com

STARTING AUDITING

1. Create journal receiver

```
CRTJRNRCV JRNRCV(user-lib/user-name001)  
AUT(*EXCLUDE)
```

2. Create journal

```
CRTJRN JRN(QSYS/QAUDJRN)  
JRNRCV(user-lib/user-name001)  
AUT(*EXCLUDE)
```

FIXED
NAME

3. Change system values

Log level
40 failures

```
CHGSYSVAL QAUDLVL VALUES(' *PGMFAIL ...')
```

```
CHGSYSVAL QAUDCTL VALUES(' *AUDLVL ')
```

Turn on audit

DSPAUDJRNE ENTYP(AF) OUTPUT(*PRINT)



Violation Type	User profile	Object name	Library name	Object type
AF A	WOEVANS	QSYSOPR	QSYS	*MSGQ
AF D	QSYS	S103478600	QSYS	*DEVD
AF D	QSYS	S103478600	QSYS	*DEVD
AF A	QUSER	ZRCRPCSPC	QTEMP	*USRSPC
AF A	QTMHH			
AF A	QTMHH			
AF A	QUSER			
AF A	WOEVA			
AF A	QUSER			
AF A	QUSER			

Violation code in audit AF entries

Violation Code	Description	Level 40 Problem
A	Not authorized	No
B	Blocked Instruction	Yes
C	Program Checksum	Yes
D	Domain Failure	Yes
J	Submit Job Failure	No
P	Profile Swap Failure	No
R	Restricted Interface	Yes
S	Sign-on information blank	Fix

Check the violation code

#3 – Remote Access

◆ Challenge

- Maintaining control over the numerous remote access points in OS/400
 - Client Access
 - File Transfer
 - Remote Commands
 - FTP
 - ODBC

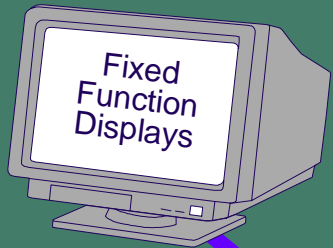
◆ Remedy

- Control object level security
- Use exit programs to limit remote access

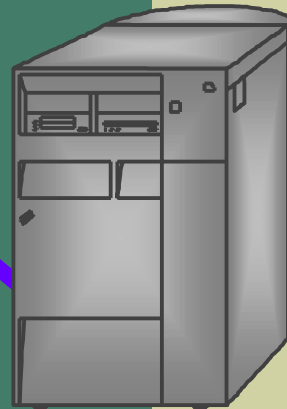


Security Has Changed

1980s



Menu Security



Today

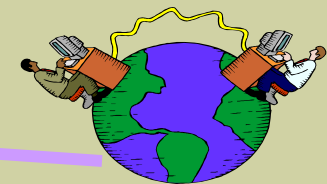
PC Users



Remote Systems



Internet



E-Commerce



Menu Security

Menu security worked when users had no other access

Menu security ineffective for today's environment

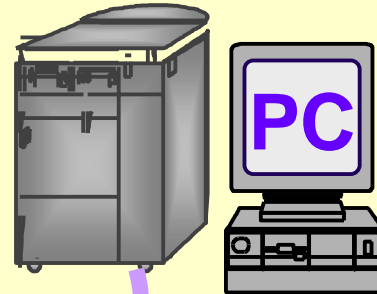
#3 Exit Programs Control Access



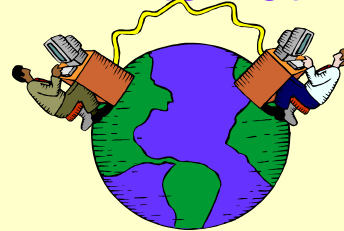
Exit Program

Exit Programs can restrict requests

Remote Systems



Internet



◆ Client Access

- File Transfer
- Remote Commands

◆ DDM (Distributed Data Management)

- File Transfer
- Remote Commands

◆ FTP

- File Transfer
- Remote Commands

◆ ODBC

◆ Telnet

◆ IFS

(Integrated File System)



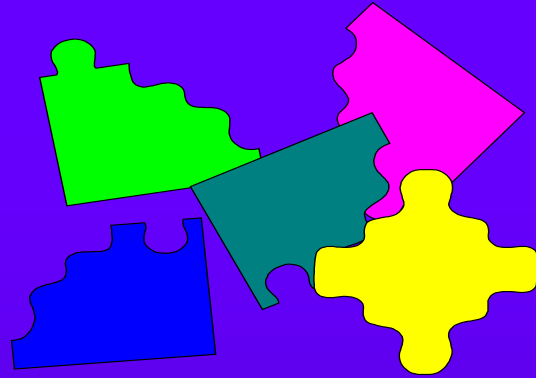
Exit Programs

- ◆ Exit programs can control actions of PC users
- ◆ Exit programs are not easy to implement
- ◆ Difficult to control Operations Navigator with exit programs

For detail go to WWW.WOEvans.com

- Exit program fundamentals article
- Comparison of vendor exit programs
- Download sample exit program code

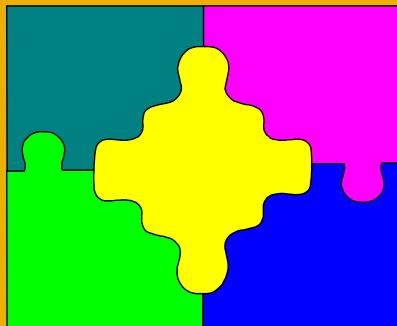
Exit Program Recommendation



- ◆ OS/400 Provides
 - Exit Points
 - Registration Facility
 - Security APIs

You must provide the programming to put the individual pieces together

Purchase exit programs



- **Software Vendors Provide**
 - ◆ Complete application that integrates IBM support into useful tool

#4 – Restricting Operations Navigator

◆ Challenge

- Operations navigator gives users powerful functions
 - Move, Rename, and Deletion of objects (if user is authorized to object)
- Operations navigator is not limited by command line (LMTCPB) or command authority

◆ Remedy

- Application Administration to limit Operations Navigator



Operations Navigator



- Management Central (51026695)
- My Connections
 - 192.168.1.11
 - Basic Operations
 - Work Management
 - Configuration and Service
 - Network
 - Security
 - Users and Groups
 - Database
 - File Systems
 - Backup
 - Application Development
 - AFP Manager
 - Tivoli IT Director

Before

- Management Central (51026695)
- My Connections
 - 192.168.1.11
 - Basic Operations
- 1026695

Application Administration restricts dangerous options

After

Application administration is used to hide Operations Navigator options

Invoking App Admin

The screenshot displays the IBM Management Central interface. On the left, a tree view shows the hierarchy: Environment: My Connections > Management Central (Achi... > My Connections > WebSphere. A context menu is open over 'WebSphere', listing various actions such as 'Explore', 'Open', 'Display Emulator...', 'Create Desktop Icon', 'Verify Connection...', 'Delete...', 'Change Password...', 'Inventory', 'Collection Services', 'Fixes', 'Users and Groups', 'Run Command...', 'Monitors', 'Application Administration', 'Send Message...', 'EZ-Setup Custom Setup', and 'Properties'. The 'Application Administration' option is highlighted. In the bottom right corner, a task list includes: 'Run a command', 'Configure Application Administration', 'EZ-Setup Custom Setup', and 'Help for related tasks'. A light blue speech bubble with a dark blue border points to the 'Application Administration' menu item and the 'Configure Application Administration' task, containing the text: 'Two ways to invoke application administration'. The main pane shows a table with columns 'Name' and 'Description' containing various system components like 'Basic Operations', 'Work Management', 'Configuration and Service', etc.

Name	Description
Basic Operations	Manage messages, printer output and printers.
Work Management	Manage jobs and server jobs.
Configuration and Service	Display system inventory, work with fixes, and collect pe...
Work	Manage TCP/IP and Internet support.
Security	Configure and manage security.
Users and Groups	Manage OS/400 users and user groups.
Database	...
Systems	...
Up	...
Education Developme	...

Two ways to invoke application administration

- Run a command
- Configure Application Administration
- EZ-Setup Custom Setup
- Help for related tasks

1 - 10 of 10 objects

Controlling Operations Navigator

Application Administration - Achillie

Select the functions or applications available to users.

Select operations allowed for *PUBLIC and *ALLOB users

AS/400 Operations Navigator | Client Applications | Host Applications

Function	Default Access	All Object Access	Customized Access
[-] Achillie in My Connections	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Basic Operations	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Messages	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Printer Output	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Printers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Jobs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Work Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Active Jobs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Server Jobs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Subsystems	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Job Queues	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Memory Pools	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Configuration and Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] System Values	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
[-] Hardware	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

IBM Default is to allow all operations navigator functions

Restrict Options for Users

Application Administration - 192.168.1.11

Select the functions or applications available to users.

AS/400 Operations Navigator | Client Applications | Host Applications

Function	Default Access	All Object Access	Customized Access
192.168.1.11 in My Connections	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Basic Operations	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Messages	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Printer Output	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Printers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Jobs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Work Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Active Jobs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Server Jobs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Subsystems	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Job Queues	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Memory Pools	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Configuration and Service	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
System Values	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Hardware	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Remove Customization

Customize

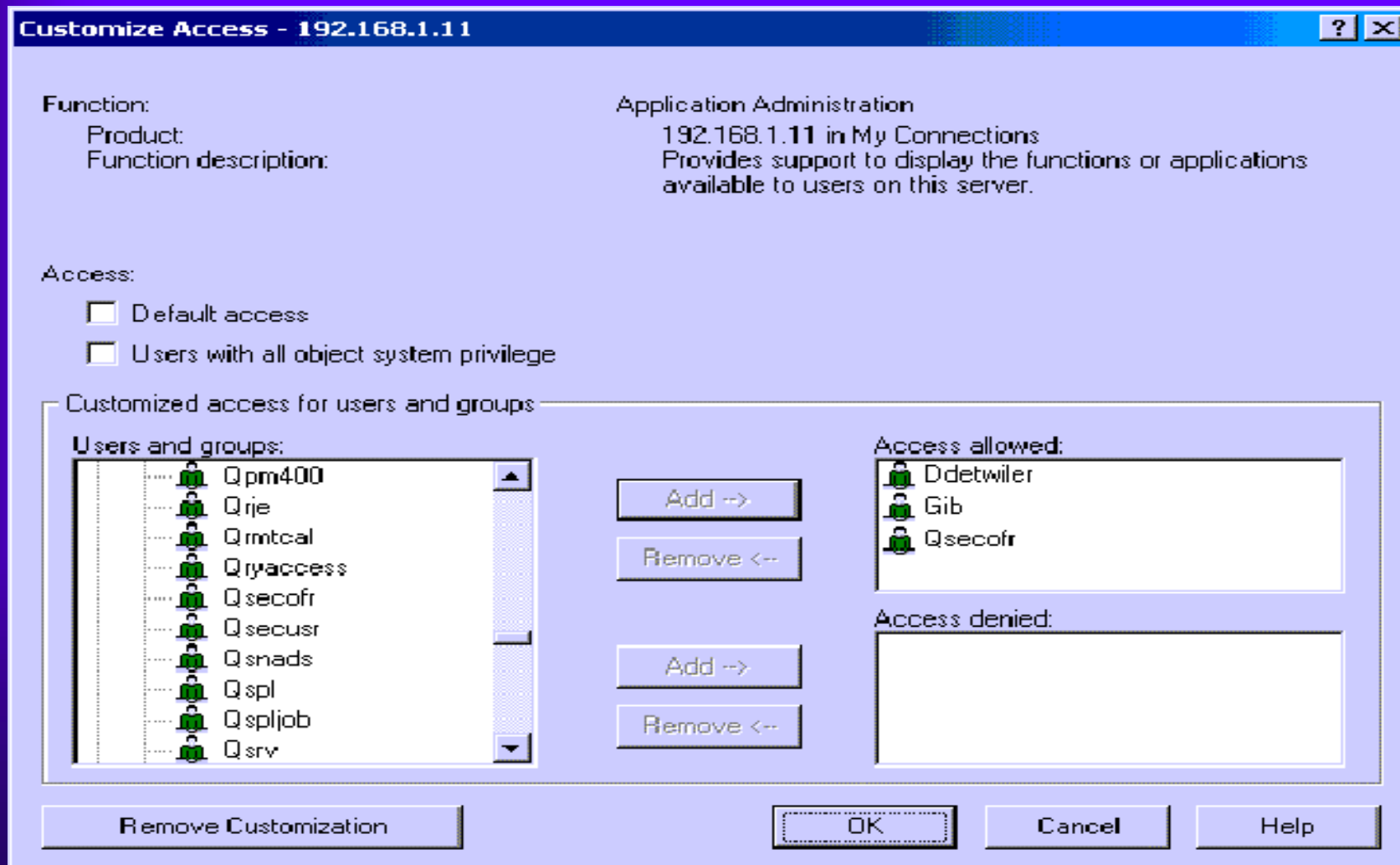
Applications ...

OK Cancel Help

Set Default access to Basic Operations

Controlling Operations Navigator

Limit users that can use Application Administration



#5 – Limiting Command Line



◆ Challenge

- Limit users to menu options
- End users should not be allowed to use CL Commands

◆ Remedy

- LMTCPB(*YES) in user profile
- Use PRTUSRPRF to find profiles with command line access

#6 – Eliminate Unused Accounts

◆ Challenge

- Keeping up with numerous personnel changes and their user profiles can be difficult
 - User profile management is time consuming
 - Updating the system for recently terminated users is frequently overlooked

◆ Remedy

- Security Tools option to find and disable inactive user profiles



#6 Profiles not signed on

GO SECTOOLS

SECTOOLS Security Tools

Select one of the following:

Work with profiles

1. Analyze default passwords
2. Display active profile list
3. Change active profile list
4. Analyze profile activity
5. Display activation schedule
6. Change activation schedule entry
7. Display expiration schedule
8. Change expiration schedule entry

Inactive user
profile check

Selection or command

===> _____

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

#7 – Excessive special authorities

◆ Challenge

Users are given too much special authority

***ALLOBJ** -- Allows access to all data

***SERVICE** – Service tools bypass security

***SPLCTL** -- Access to all spool files

***SECADM** – Manage user profiles

• Remedy

- Use PRTUSRPRF (Print User Profile)



User Profile Information

PRTUSRPRF

User	Group	*ALL	*AUD	SYS	*JOB	*SAV	*SEC	*SER	*SPL	User
Profile	Profiles	OBJ	IT	CFG	CTL	SYS	ADM	VICE	CTL	Class
DENON	*NONE	X	X	X	X	X	X	X	X	*SECOFR
FENDT	*NONE									*USER
HOFFMAN	*NONE									*USER
HOLT	QPGMR				X	X				*PGMR
HOOPES	*NONE				X	X			X	*SYSOPR
KLIMA	QPGMR				X	X				*PGMR
LAURENT	*NONE									*USER

* * * truncated output * * *

#8 – Elimination of Trivial Passwords



◆ Challenge

- Insure that passwords are not compromised
- Avoid trivial passwords such as password same as the user profile

◆ Remedy

- System values for expiration and content rules
- Security tools ANZDFTPWD to check for password same as user profile name

#8 – Eliminate of Trivial Passwords

System Value	Description	Recommendation
QPWDLVL	Type of Password	0
QPWDMINLEN	Minimum Length	10
QPWDMAXLEN	Maximum Length	>=6
QPWDLMTREP	Limit repeating char	2=no adj duplicates
QPWDRQDDIF	Limit pwd repetition	1-5 at least 10 differ
QPWDRQDDGT	Require Digit	1 = yes
QPWDLMTAJC	Prevent adjacent digits	0 = no
QPWDPOSDIF	Positional difference	0 = no restriction
QPWDVLDPGM	Validation Program	*NONE

#8 – Find Trivial Passwords

GO SECTOOLS

SECTOOLS

Security Tools

Select one of the following:

Work with profiles

1. Analyze default passwords
2. Display active profile list
3. Change active profile list
4. Analyze profile activity
5. Display activation schedule
6. Change activation schedule entry
7. Display expiration schedule
8. Change expiration schedule entry

Selection or command

===> _____

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Password =
Profile

New profiles that
have never
signed on or
reset passwords

#9 – Authority to User Profile

◆ Challenge

- The *PUBLIC authority to for user profiles should be *EXCLUDE
- If other users have access to a user profile they can submit jobs as that user

◆ Remedy

- Security tools PRTPUBAUT to find profiles with excessive authority



Authority to User Profiles



FRED

Object Authority
***PUBLIC *USE**

When users have *USE
authority to other
profiles Jobs can be
submitted as other users

SBMJOB USER(FRED) CMD(CL command)

Recommend

**User profiles public authority = *EXCLUDE
to prevent running jobs as other users**

Check Authority to User Profiles

PRT PUBAUT OBJTYPE(*USRPRF)

```
Publicly Authorized Objects (Full Report)

Object type . . . . . : *USRPRF
Specified library . . . . . : QSYS

Auth -----Object-----Data-----
Libr Object Owner List Authority Opr Mgt Exist Alter Ref Read Add Upd Dlt Exec
QSYS FRED QSECOFR *USE X X
QSYS QDBSHR QSYS USER DEF X X
QSYS QDBSHRDL0 QSYS USER DEF X X
QSYS QSPJOB QSYS *USE X X
QSYS QTMPLFD QSYS USER DEF X

*****
E N D O F L I S T I N G * * * * *
```

Profiles shown are OK

Revoke *PUBLIC authority from other profiles

#10 – Inappropriate Object Authority

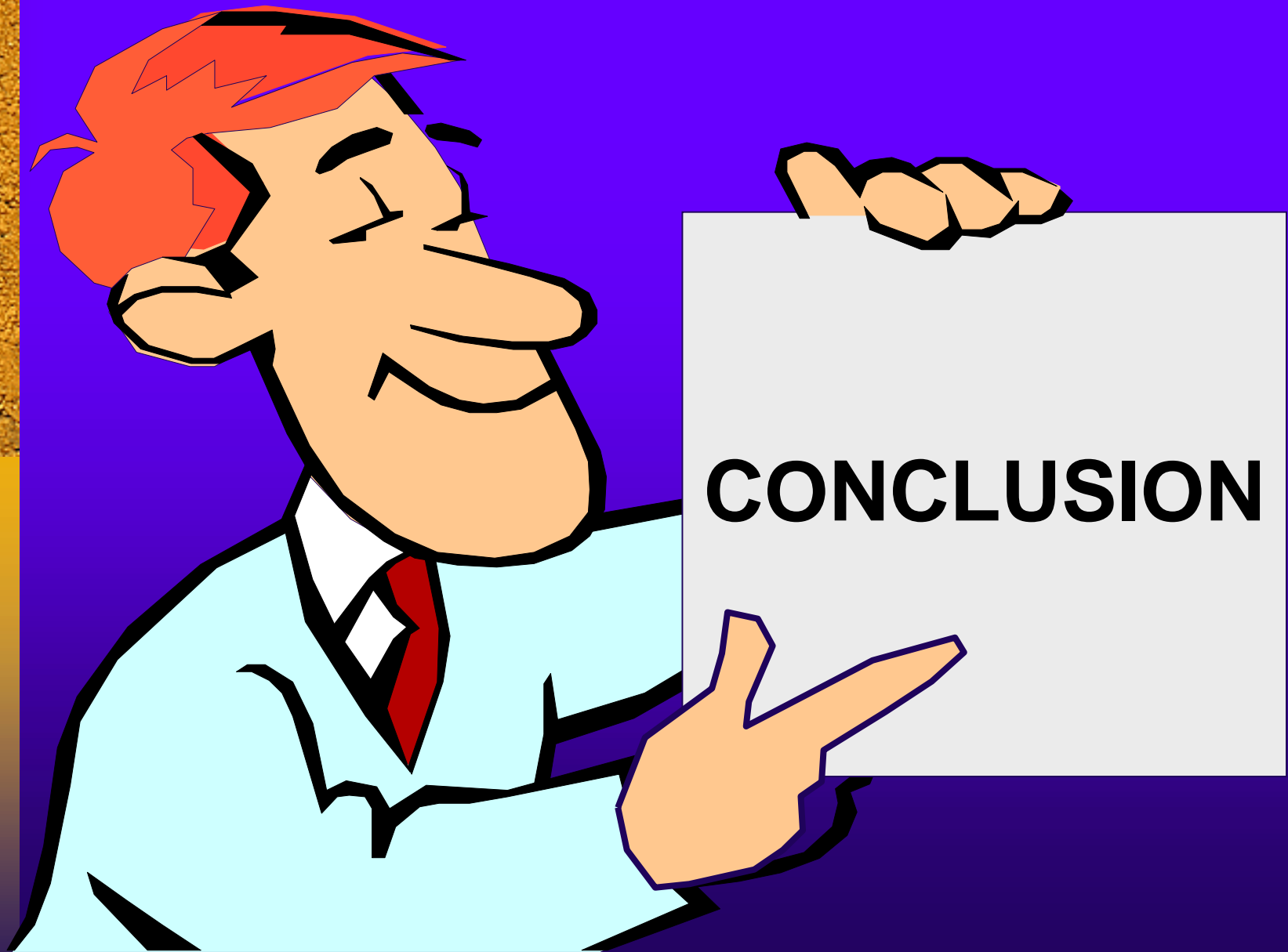
◆ Challenge

- Users may be able to view and access OS/400 libraries and objects
 - Improper permissions may be set for the “*PUBLIC” users
 - Detecting changes for PC users accessing the system via OpsNav

◆ Remedy

- PRTPUBAUT (Print Public Authority)
- PRTPRVAUT (Print Private Authority)






Action Plan



- ✓ Create a security policy to define security goals
- ✓ Move to security level 40
 - If audit journal indicates no application problems
- ✓ Control PC access
 - Implement exit programs to control FTP, File Transfer, Remote Commands
 - Limit Operations Navigator (Application Administration)

Action Plan



✓ User Profiles

- Eliminate unused accounts
- Restrict command line for end users
- Avoid use of trivial passwords
- Limit powerful special authority

***ALLOBJ *SECADM *SPLCTL *SERVICE**

✓ Verify *PUBLIC authority to user profiles is *EXCLUDE except for the profiles:

QDBSHR QBSSHRDLO QSPLJOB QTMPLPD

✓ Limit *PUBLIC authority to objects and libraries



QUESTIONS

If you have additional questions or want more information please contact me

Wayne O. Evans

WOEvans@AOL.com

Visit my web site

<http://WWW.WOEvans.COM>