

AS/400 & iSeries

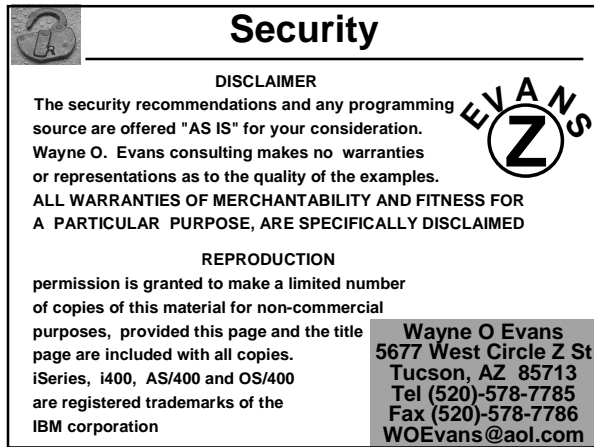
SECURITY IMPLEMENTATION

Tips and Techniques

© Wayne O. Evans Consulting, Inc 2001

Presented by
Wayne O. Evans

1



Security

DISCLAIMER

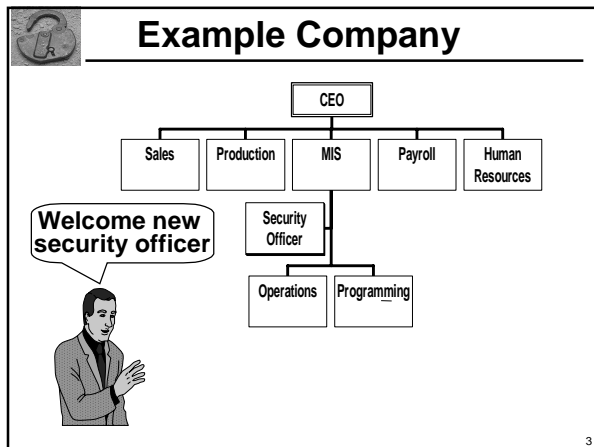
The security recommendations and any programming source are offered "AS IS" for your consideration. Wayne O. Evans consulting makes no warranties or representations as to the quality of the examples. **ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE SPECIFICALLY DISCLAIMED**

REPRODUCTION

permission is granted to make a limited number of copies of this material for non-commercial purposes, provided this page and the title page are included with all copies. iSeries, i400, AS/400 and OS/400 are registered trademarks of the IBM corporation

EVANS

Wayne O Evans
5677 West Circle Z St
Tucson, AZ 85713
Tel (520)-578-7785
Fax (520)-578-7786
WOEvans@aol.com



Example Company


CEO

- Sales
- Production
- MIS
 - Security Officer
 - Operations
 - Programming
- Payroll
- Human Resources


Welcome new security officer

3

Bad Start



I want you to secure the system




Where do I start?
 What are the important business resources?
 How much security is enough?


IT IS VERY DIFFICULT TO SECURE A SYSTEM UNLESS YOU UNDERSTAND THE OBJECTIVE

4

Good News



I want you to implement the company security **POLICY**




GOOD Now I have a starting point

The **POLICY** should explain the expectations for security not the details

QUESTIONS
 Is the policy current?
 Does management support the policy?


5

Security Policy



◆ You should never attempt to build a house with out a plan

You might be able to get started but the long term results can easily result in unstructured mess



Like a house plan a security policy provides the direction for the building of security on the system

Security Policy = Plan for Security

6



Security Policy

A written security policy provides a basis for security decisions

- When users do not like some security changes allows the security officer to say

"It is not my rules, I am simply implementing management requests"



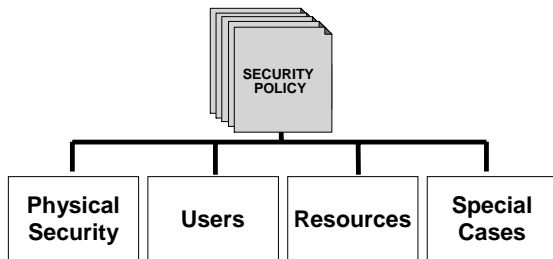
- Reduces changes to security design based on the latest management hot button
- Forces management to think about and set security expectations before exposures happen

7



Security Policy

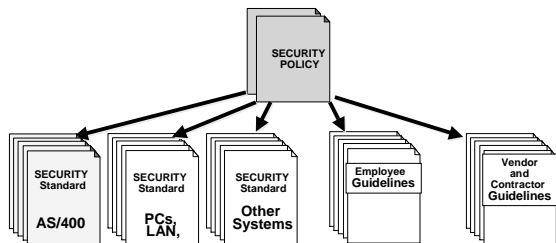
The security policy is a general statement of the corporate security practices



8




Standards and Guidelines



Security Standards are an interpretation of the security policy for a computer system


Security Guidelines are an interpretation of the security policy for a user actions

9

 **Policy and Standard**


<p>Policy</p> <p>The 10 Commandments Thou shall not steal</p> <p>USER ACCESS Prevent unauthorized access to the system</p> <p>High Level Statements</p>	<p>Standard</p> <p>Civil Justice Code Car theft is a felony punishable by ...</p> <p>USER ACCESS After three consecutive sign-on failures, the system will: * Vary off the device * Disable the user profile</p> <p>Detail Statements</p>
---	---

10

 **Policy Standards Guidelines**

<p>Policy</p> <p>USER ACCESS Prevent unauthorized access to the system</p>	
<p>AS/400 Standard</p> <p>USER ACCESS After three consecutive sign-on failures, the system will: * Vary off the device * Disable the user profile</p>	<p>User Guideline</p> <p>USER ACCESS Protect your password so that others can not sign-on using your access DO NOT SHARE YOUR PASSWORD with ANYONE</p>

11

 **Examples**

→

- ◆ Reset Profile Passwords
- ◆ Selective Inactive Workstation Timeout
- ◆ Lost Security Officer Password Recovery
- ◆ User Profile Administration
- ◆ Controlling *ALLOBJ Users
- ◆ Modify Sign-on Display
- ◆ Limit Spool File Access
- ◆ Limiting Client Access Functions

12



Limit Password Guessing

```
CHGSYSVAL QMAXSIGN '3'  
CHGSYSVAL QMAXSGNACN '3'
```

After 3 failed attempts disable
➤ user profile
➤ device

PROBLEM

Provide a way so that the chief operator can enable profiles

USER ACCESS

After three consecutive sign-on failures, the system will:
* Vary off the device
* Disable the user profile

SPECIAL CASE

Operations will be allowed to activate the device and profile

13



Enable User Profile

Problem 1
Provide a way so that the chief operator can enable profiles

```
ENABLE USRPRF(GLOOP)
```

```
PGM &USER  
DCL &USER *CHAR(10)  
CHGUSRPRF USRPRF(&USER)+  
STATUS(*ENABLED)  
ENDPGM
```

```
*PGM  
Owner-QSECOFR
```

PROBLEM

If users forget their password, this program is not adequate

14



Enable User Profile


Problem 2
Provide a way to handle lost user passwords

```
PGM &USER  
DCL &USER *CHAR(10)  
CHGUSRPRF USRPRF(&USER) +  
PASSWORD(&USER) +  
STATUS(*ENABLED) +  
PWDEXP(*YES)  
SNDPGMMSG TOMSGQ(secofr) +  
MSG('User ' || &USER || ' reset ')  
ENDPGM
```

Expire password to force user change

Send message or write to audit journal to alert the security officer to changes

15

 **Enable User Profile**

PROBLEM 3
The operator can't run program

CHGUSRPRF command requires *SECADM and authority to the profile or *ALLOBJ

Should not give operators this level of access

SOLUTION
Use program adoption to give operator need access

CRTCLPGM ENABLE
USRPRF(*OWNER)


OR

CHGPGM ENABLE
USRPRF(*OWNER)

ADOPT
OWNER

*PGM
Owner-QSECOFR

16

 **Enable User Profile**


PROBLEM 4
Discovered that anyone could call program
WHY?
Default *PUBLIC authority is *CHANGE

Need to limit access to the chief operator

SOLUTION
Use AS/400 security to limit access to the chief operator

- Revoke *PUBLIC authority
- Grant access to specific users
 - Create authorization list
 - Secure program and command

17

 **Enable User Profile**

Revoke *PUBLIC

GRTOBJAUT ENABLE OBJTYPE(*pgm)
USER(*PUBLIC) AUT(*EXCLUDE)

GRTOBJAUT ENABLE OBJTYPE(*cmd)
USER(*PUBLIC) AUT(*EXCLUDE)

Create authorization list

CRTAUTL LIST1 AUT(*EXCLUDE)

Add users

ADDAUTLE AUTL(LIST1)
USER(CHIEFOPER) AUT(*USE)

Add objects

GRTOBJAUT ENABLE OBJTYPE(*pgm)
AUTL(LIST1)

GRTOBJAUT ENABLE OBJTYPE(*cmd)
AUTL(LIST1)

18



Enable User Profile

Create authorization list

```
CRTAUTL LIST1 AUT(*EXCLUDE)
```

Add users

```
ADDAUTL AUTL(LIST1)  
USER(CHIEFOPER) AUT(*USE)
```

Create objects and add to AUTL

```
CRTCLPGM ENABLE USER(*OWNER)  
AUT(LIST1)  
CRTCMD ENABLE PGM(ENABLE)  
AUT(LIST1)
```

19



Authorization List Advantages

QUESTION

WHY use an authorization list rather than individually granting users access

ANSWER

Private authorization could be secured by granting individual operators access to both the command and program

I anticipate that other operators will have similar needs. It will be less work to add new users to the authorization list

20



Authorization List or Group Profile

QUESTION

WHY use an authorization list rather than a group profile?

ANSWER

Other individuals may be in the operator group.
Only the CHIEF operator should have this function.

21



Enable User Profile

Summary

- ✓ Controlling number of invalid attempts to enter password (prevent hackers)
- ✓ Enabling of user profile by CL program
- ✓ Use of program adoption of authority
- ✓ Use of authorization list to secure objects

22



Enable User Profile

PROBLEM 5

The program shown could be used to change the password of a security officer

SOLUTION

Add code to retrieve the user profile and prevent changes to profiles that have powerful special authorities
*ALLOBJ, *SERVICE, *AUDIT, *SECADM

The RTVUSRPRF command or the API QSYRUSRI can retrieve special authority

23



Examples



- ◆ Reset Profile Passwords
- ◆ Selective Inactive Workstation Timeout
- ◆ Lost Security Officer Password Recovery
- ◆ User Profile Administration
- ◆ Controlling *ALLOBJ Users
- ◆ Modify Sign-on Display
- ◆ Limit Spool File Access
- ◆ Limiting Client Access Functions

24



Time Out Inactive Terminals

STANDARD
TIME OUT
work-station
inactive for 30
minutes should
return to the
sign-on screen

OS/400 has system
values to active
timeout of inactive
workstations.

CHGSYSVAL QINACTIV '30'
CHGSYSVAL QINACTMSGQ '*DSCJOB'

PROBLEM

The work-station in machine
room keeps getting signed off

25

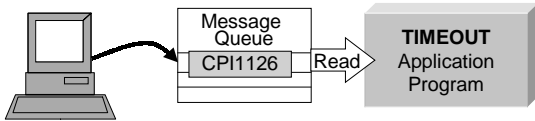


Time Out Inactive Terminals

**Need to have different timeout
rules for some workstations**

SOLUTION

1. OS/400 sends a message on workstation
timeout.
2. Have a program handle the timeout



26



Time Out Inactive Terminals

- Create message queue for time-out messages

CRTMSGQ TIMMSG

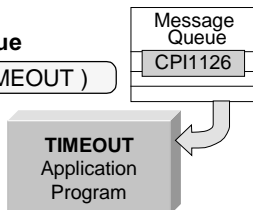
- Direct time out messages to queue

CHGSYSVAL QINAJOBMSGQ TIMMSG

- Start a never-ending job to
process messages on queue

SMBJOB CMD(CALL TIMEOUT)

Add job start to initial
start up procedures



27



Examples

- ◆ Reset Profile Passwords
- ◆ Selective Inactive Workstation Timeout
- ➔ ◆ Lost Security Officer Password Recovery
- ◆ User Profile Administration
- ◆ Controlling *ALLOBJ Users
- ◆ Modify Sign-on Display
- ◆ Limit Spool File Access
- ◆ Limiting Client Access Functions

28



Recovery from Lost Password

The security officer can assign users a new password

```
CHGUSRPRF USRPRF(xxx)
PASSWORD(XXX)
PWDEXP(*YES)
```

PASSWORDS

Provide a method to recover from lost passwords



PROBLEM
What if the security officer password is lost?

29



Lost Security Officer Password

1. Use Dedicated Service Tools to reset password

- Change DST Password
1. Change DST basic capability password
 2. Change DST full capability password
 3. Change DST security capability password
 4. Reset system default password
- Selection ___

DST recovery assumes you know the DST password

2. IBM assistance (service fee)

3. Have a back-up plan

30

Recovery from Lost Password

Give CEO a method to change the password of the security officer

```
CRTUSRPRF CEO USRCLS(*SECOFR)
PASSWORD(---) INLPGM(FIXIT) LMTCPB(*YES)
```

```
PGM
CHGUSRPRF ?*USRPRF(QSECOFR)
??PASSWORD( )
STATUS(*ENABLED)
PWDEXP(*YES)
SIGNOFF
ENDPGM
```

Change User Profile

User Profile QSECOFR
Password

31

Examples

- ◆ Reset Profile Passwords
- ◆ Selective Inactive Workstation Timeout
- ◆ Lost Security Officer Password Recovery
- ➔ ◆ User Profile Administration
- ◆ Controlling *ALLOBJ Users
- ◆ Modify Sign-on Display
- ◆ Limit Spool File Access
- ◆ Limiting Client Access Functions

32

User Profile Administration

Security Officer Duties

- ◆ Create group profiles
- ◆ Create administrator profiles
- ◆ Create administrator tools
- ◆ Train and advise administrators

Security Administrator

- ◆ Create new user profiles
- ◆ Reset passwords
- ◆ Delete individual users

33

User Profile Administration

User Profile Sec Offcr The security officer has *ALLOBJ and *SECADM and can access all profiles

User Profile Admin With *SECADM the administrator profile can only access users in their area.
WHY? The administrator is authorized to the user profiles they created

Mfg

Sales

Acct

34

Set Up User Profiles

Security Officer Actions

User Profile Sec Offcr

CRTUSRPRF GRPMFGADM
 PASSWORD(*none)
 SPCAUT(*SECADM)

CRTUSRPRF GRPMFG
 PASSWORD(*none)

CRTUSRPRF MFGxxxxxxx
 PWDEXP(*YES) USRCLS(*USER)
 AGCDTA(MFG) CURLIB(MFGLIB)
 GRPPRF(GRPMFG)
 OWNER(*GRPPRF)
 SUPGRPPRF(GRPMFGADM)

Additional group profile gives user security administration capabilities

35

Set Up User Profiles

Security Officer Actions

User Profile Sec Offcr

CHGOBJOWN GRPMFG
 OBJTYPE(*USRPRF)
 NEWOWN(GRPMFGADM)

CHGOBJOWN GRPxxxxxx
 OBJTYPE(*USRPRF)
 NEWOWN(GRPMFGADM)

Change user profile owner to administration group

36

Enroll New User in Group

Security Administrator

User Profile Admin

```

CRTUSRPRF MFGxxxxxxx
PASSWORD(xxx)
PWDEXP(*YES)
GRPPRF(GRPMFG)
OWNER(*GRPPRF)
  
```

Owner of user profiles

```

CHGOBJOWN MFGxxxxxxx
OBJTYPE(*USRPRF)
NEWOWN(GRPMFGADM)
  
```

Repeat steps for every user in group

37

Simplify Administration

Hide security complexity by using an administrator screen interface

Security Administration

- 1.
- 2.
3. Add a new user
4. Reset password
5. Remove user

Select option 3

```

PGM
DCLF ADDUSER
SNDRCVF
CRTUSRPRF ....
CHGOBJOWN ....
ENDPGM
  
```

ADD USER

Name. . . : _____

Text. . . : _____

38

Examples

- ◆ Reset Profile Passwords
- ◆ Selective Inactive Workstation Timeout
- ◆ Lost Security Officer Password Recovery
- ◆ User Profile Administration
- ◆ Controlling *ALLOBJ Users
- ◆ Modify Sign-on Display
- ◆ Limit Spool File Access
- ◆ Limiting Client Access Functions

39

Controlling *ALLOBJ Users

Standard

Programming staff should not have *ALLOBJ special authority

Standard

Actions of users with *ALLOBJ special authority should be logged

Standard

Limit where users with *ALLOBJ authority can sign-on

◆ *ALLOBJ authority allows users access to all objects.

User Can Delete Production Data

Strategy: Remove *ALLOBJ authority from user profile to prevent accidental access

40

Logging Commands

LOG COMMANDS

1. Turn on command audit in user profile
2. Swap user profile to activate changes
3. Show command entry and receive command
`SNDMSG *RQS`
4. Run the command
`CALL QCMDEXEC`
5. Record the commands used in the audit journal
`SNDJRNE`

CL command

↙

QCMDEXEC

↔

QAUDJRN

↔

Journal Receiver

41

Controlling an *ALLOBJ User

STRATEGY: Create a command LOGCMD that adopts *ALLOBJ access and logs commands entered in audit journal

1. Create user profile with *ALLOBJ special authority

`CRTUSRPRF OWNALLOBJ SPCAUT(*ALLOBJ) PASSWORD(*NONE)`
2. Create authorization to control LOGCMD adopted access

`CRTAULT LOGCMD AUT(*EXCLUDE)`

42



Controlling an *ALLOBJ User

3. Create program that adopts authority

```
CRTCLPGM LOGCMDA USRPRF(*OWNER)
AUT(LOGCMD)
```
4. Create LOGCMD command

```
CRTCMD LOGCMD PGM(LOGCMDA)
AUT(LOGCMD)
```
5. Change ownership of objects

```
CHGOBJOWN LOGCMD OBJTYPE(*CMD)
NEWOWN(OWNALLOBJ)
```

```
CHGOBJOWN LOGCMDA OBJTYPE(*PGM)
NEWOWN(OWNALLOBJ)
```
6. Restrict *ALLOBJ user sign-on

```
CHGSYSVAL QLMTSECOFR VALUE('1')
```

43



Examples

- ◆ Reset Profile Passwords
- ◆ Selective Inactive Workstation Timeout
- ◆ Lost Security Officer Password Recovery
- ◆ User Profile Administration
- ◆ Controlling *ALLOBJ Users
- ➔ ◆ Modify Sign-on Display
- ◆ Limit Spool File Access
- ◆ Limiting Client Access Functions

44



Customized Sign-on Screen

Sign On

	System : xxxxxxx
	Subsystem : QINTER
	Display : PADEV0023

User : _____

Password : _____

This area used for message to users

THIS MESSAGE WILL NOT BE DISPLAYED IF THE USER
IS NOT AUTHORIZED TO RECEIVE IT FROM THE SYSTEM

Restricted access
warning message

WARNING
Access to his system is restricted DO NOT PROCEED UNLESS AUTHORIZED.
We reserve the right to fully pursue criminal and civil penalties.
Users of this system consent to monitoring.

45



Customized Sign-on Screen

Standard

Provide a warning banner on sign-on screen to discourage hackers

1. Copy DDS source of sign-on display QDSIGNON in QGPL/QDDSRC to you own file
2. Use SEU to edit source (see result on next screen)
 - A. Do not delete any fields hide extra fields by making them non-display
 - B. Add additional warning text
 - C. Add message fields for messages to users
3. Create display file be sure to specify MAXDEV(256)

```
CRTDSPF  DSPG(QSYS/MYSIGNON) MAXDEV(256)
          SRC(...) SRCMBR(...) AUT(*CHANGE)
```

46



Customized Sign-on Screen

4. Create Message file and add messages

```
CRTMSGF  MSGF(QSYS/SGNMSGF) AUT(*USE)
```

```
ADDMSGD  MSGF(QSYS/SGNMSGF)
          MSGID(SGN0001) MSGTXT(' ')
```

Add other messages

```
ADDMSGD  MSGF(QSYS/SGNMSGF)
          MSGID(SGN0005) MSGTXT(' ')
```

5. Use screen design aid to test display file

47



Customized Sign-on Screen

6. Make a copy of QINTER subsystem

```
CRTDUPOBJ  OBJ(QINTER) OBJTYPE(*SBSD)
            NEWOBJ(MYQINTER)
```

7. Modify copy to use new display file

```
CHGSBSD  SBSD(MYQINTER)
          SGNDSPF(MYSIGNON)
```

8. Start new subsystem

```
STRSBSD  MYQINTER
```

48



Customized Sign-on Screen

9. Create Display file used to edit sign-on messages

```
CRTDSPF DSPF(EDTSGNMSGF)
```

10. Create program used to edit sign-on messages

```
CRTCLPGM PGM(CHGSGNON) AUT(*EXCLUDE)
```

11. Call program to edit sign-on messages

```
CALL CHGSGNON
```

49



Examples

- ◆ Reset Profile Passwords
- ◆ Selective Inactive Workstation Timeout
- ◆ Lost Security Officer Password Recovery
- ◆ User Profile Administration
- ◆ Controlling *ALLOBJ Users
- ◆ Modify Sign-on Display
- ◆ Limit Spool File Access
- ◆ Limiting Client Access Functions



50



Control SPOOL output

PLAN

- Limit operator and programmer access
 - Display
 - Copy
 - Moving
 - Sending

Standard

- Limit access to sensitive printed output such as:
- Payroll Checks
 - Human Resources
 - Credit Card Pins

IMPLEMENTATION

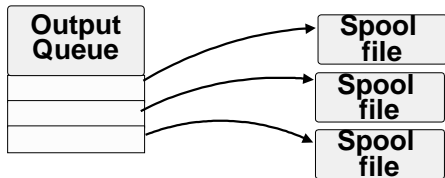
1. Can not use access control on individual Spool files
"Spool files are not objects"
2. Use of spool queue security options

51



Securing Spool Files

- Spool files can not be secured
- Securing output queues limits access to spool files

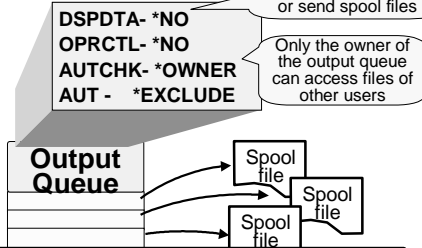


52



Securing Spool Files

- Securing output queues limits access to spool files



CAUTION: Users with *SPLCTL authority can access any spool file

53



Limit Spool Files a User Can View

The WRKSPLF command shows a user their spool files

```
WRKSPLF
SELECT(*CURRENT)
```

Guideline
Users can only view their own spool files

User Menu

```

1 xxxxxxxxxxxxxxxx
2 xxxxxxxxxxxxxxxx
3 View output
4 xxxxxxxxxxxxxxxx
  
```

Option 3

```
WRKSPLF
SELECT(*CURRENT)
```

```
WRKSPLF
```

54

Limit Spool Files a User Can View

User Menu

```

1 xxxxxxxxxxxxxxxx
2 xxxxxxxxxxxxxxxx
3 View output
4 xxxxxxxxxxxxxxxx

```

Option 3 issues

WRKSPLF
SELECT(*CURRENT)

WRKSPLF

PROBLEM

- Users have discovered a way to view other queues

55

Limit Spool Files a User Can View

WRKSPLF USER(*CURRENT)

Work with All Spooled Files

Type options, press Enter.
 1=Send 2=Change 3=Hold 4=Delete 5=Display 6=Release
 7=Messages 8=Attributes 9=Work with printing status

Opt	File	User	Queue	User Data	Sts
-	xxxxxxx	xxxxxxx	xxxxxxx	xxxxxxx	xxx
-	xxxxxxx	xxxxxxx	xxxxxxx	xxxxxxx	xxx
-	xxxxxxx	xxxxxxx	xxxxxxx	xxxxxxx	xxx

F22 can show files of other users

Parameters for options 1, 2, 3 or command
 ==>>
 F3=Exit F10=View3 F11=View2 F12=Cancel F22=Printers

56

Limit Spool Files a User Can View

PROBLEM

IBM menu options allow users to view other queues

WRKSPLF USER(*CURRENT)

Work with All Spooled Files

Type options, press Enter.
 1=Send 2=Change 3=Hold 4=Delete 5=Display 6=Release
 7=Messages 8=Attributes 9=Work with printing status

Opt	File	User	Queue	User Data	Sts
-	xxxxxxx	xxxxxxx	xxxxxxx	xxxxxxx	xxx
-	xxxxxxx	xxxxxxx	xxxxxxx	xxxxxxx	xxx
-	xxxxxxx	xxxxxxx	xxxxxxx	xxxxxxx	xxx

Parameters for options 1, 2, 3 or command
 ==>>
 F3=Exit F10=View3 F11=View2 F12=Cancel F22=Printers

SOLUTION

Use system security to restrict the WRKWTR command

- Most users restricted
- Selected users given command

57

Securing WRKWTR Command

Revoke *PUBLIC
GRTOBJAUT
QSYS/WRKWTR OBJTYPE(*cmd)
USER(*PUBLIC) AUT(*EXCLUDE)

Create authorization list
CRTAUTL WRKWTR AUT(*EXCLUDE)

Add users
ADDAUTLE AUTL(WRKWTR)
USER(USER1 USER2)
AUT(*USE)

Secure objects
GRTOBJAUT QSYS/WRKWTR
OBJTYPE(*cmd) AUTL(WRKWTR)

***EXCLUDE
*PUBLIC *USE**

WRKWTR

USER PROFILE	AUTH ORITY	AUTL MGT
EVANS	*ALL	X
USER1	*USE	
USER2	*USE	
*PUBLIC	*EXCLUDE	

WRKWTR *CMD

58

Examples

- ◆ Reset Profile Passwords
- ◆ Selective Inactive Workstation Timeout
- ◆ Lost Security Officer Password Recovery
- ◆ User Profile Administration
- ◆ Controlling *ALLOBJ Users
- ◆ Modify Sign-on Display
- ◆ Limit Spool File Access
- ◆ Limiting Client Access Functions

59

Restricted Use of Client Access

Problem
Client Access has powerful file transfer functions that can be used to modify production data

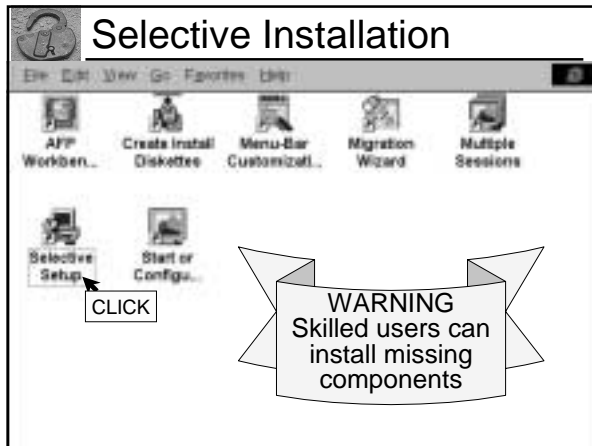
Solution
Hide or block access to PC functions

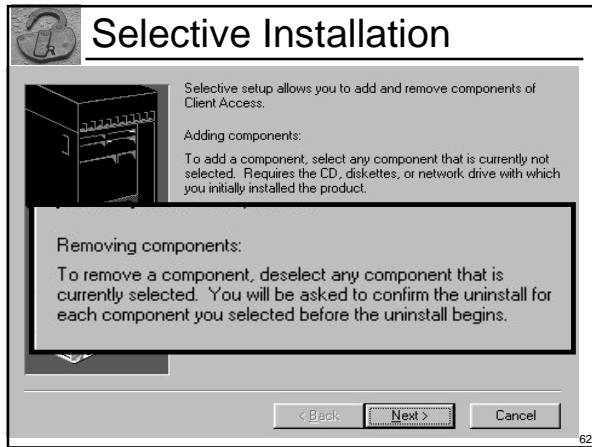
Methods

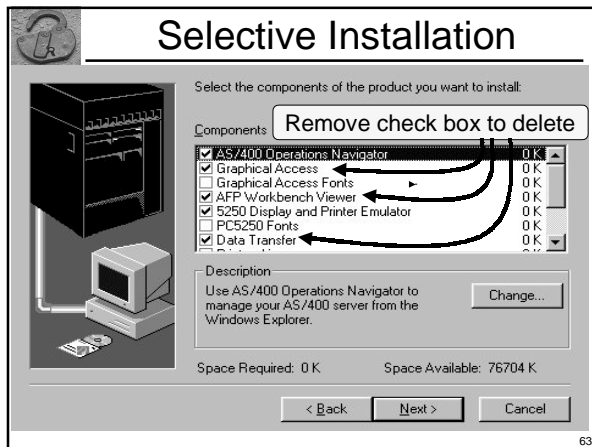
1. Selective installation
2. Exit Programs
3. Application Administration

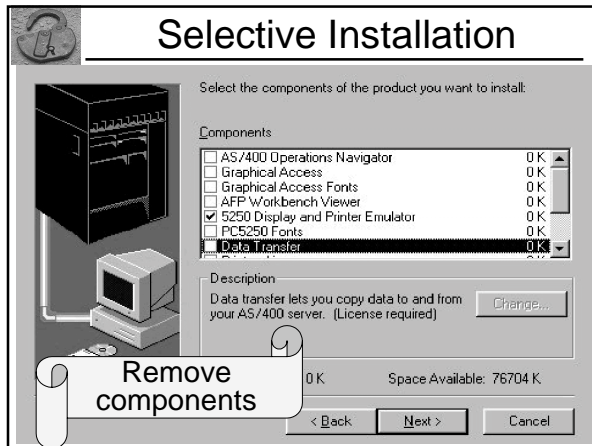
Standard
Prevent access to PC functions for end users

60









Exit Programs

Exit Program Exit programs are installation provided programs used to supplement security

Actions often performed in exit programs:

- Monitor user activity
- Modify user requests
Assign user profile to anonymous sign-on
- Review request to determine if request meets installation rules
- Reject requests that do not meet installation rules

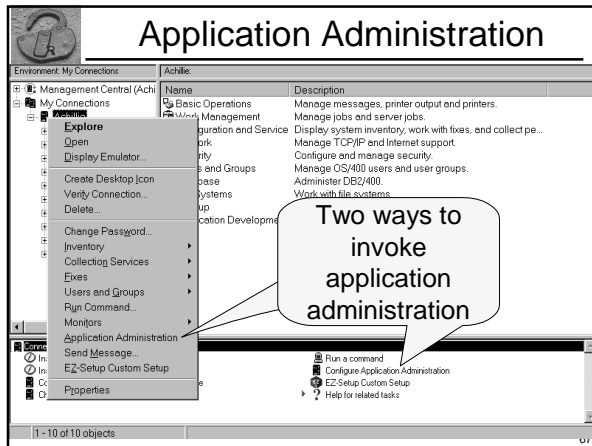
65

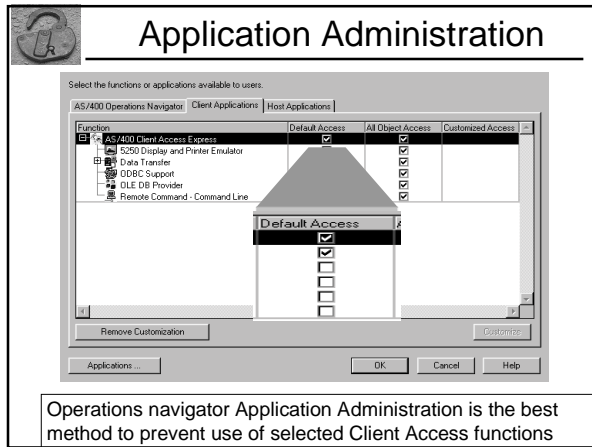
Exit Programs

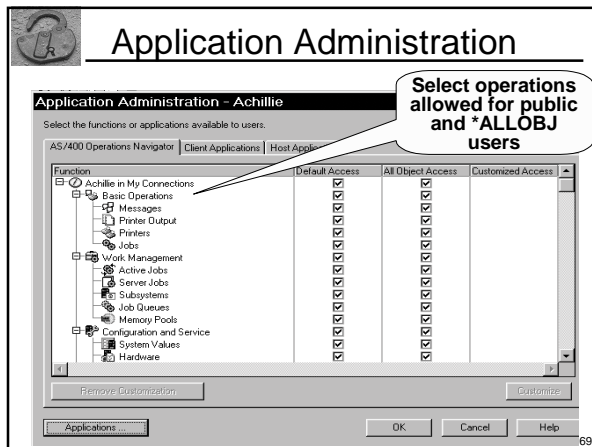
1. PC or another system generates a request
2. Server called to process request
3. Server calls "exit program" to validate request
4. Server rejects or processes the request

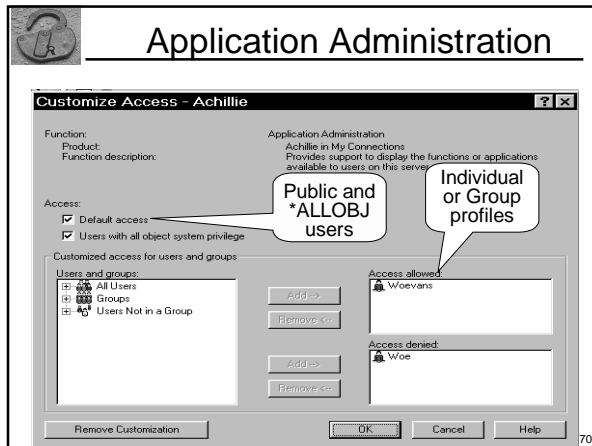
- ◆ Other sessions give exit program detail
- ◆ Creating exit programs is NOT simple
- ◆ I recommend purchase of third party vendor exit programs

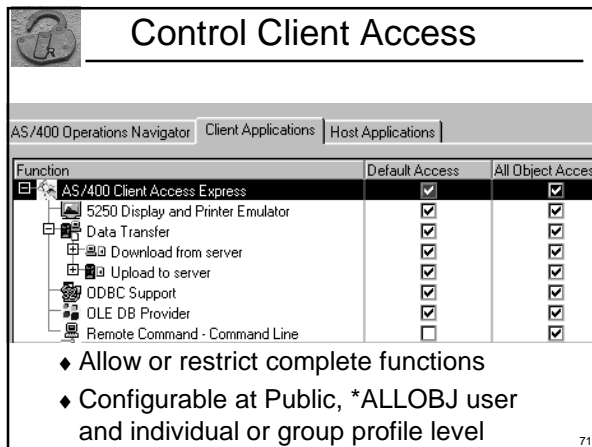
66

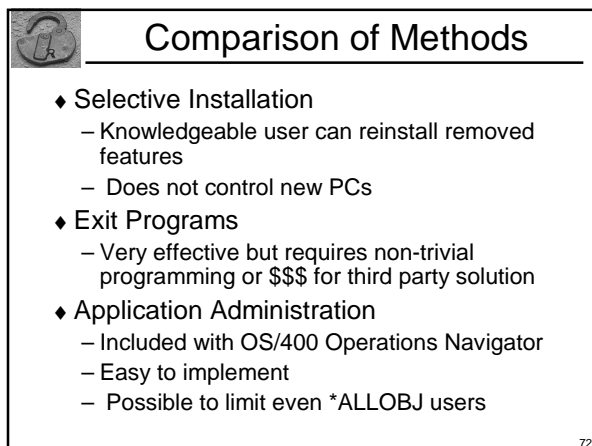














QUESTIONS

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

Phone (520) 578-7785
Fax (520) 578-7786
WOEvans@AOL.com
WWW.WOEvans.com

73
