“Ladies & Gentlemen…

Introducing **Object-Level Security”**

helpsystems

Let us help you Build a Better IT™

Today's Speaker

ROBIN TATAM, CISM CPFA CPSP CTMA PCI-P

Global Director of Security Technologies

IBM CHAMPION

robin.tatam@helpsystems.com

@robintatam

Certified for IBM | Power Systems

PCI Security Standards Council

CISM Certified Information Security Manager

COMMON SUBJECT MATTER EXPERT

Certified Professional Forensic Analyst
By Network Intelligence

Certified Payment Security Practitioner
By Network Intelligence

Certified Threat & Malware Analyst

Why bother with security?

It's all about the data residing on your systems.

The data is a corporate asset and must be secured appropriately.

helpsystems

Security Involves Evaluating Risk

Scope of the Risk

Determine scope based on the type of data and who has access to it

Business Impact

Cost to the organization should the data be lost or stolen, not available, or simply not accurate

Core Components of IBM i Security

Users

User profile settings

Object Authorities

Access to libraries, directories, and their objects

System Values

Security-relevant global settings

helpsystems

First Step or Last Step?

Object Level Security is the ‘Gold Standard’ of Security on IBM i

Often easier than people think

Is respected by all access methods

Definitive in an audit

Tools to help as of v7.3

Not the easiest concept to grasp

Not flexible to different interfaces

Other options may be quicker to implement

Doesn’t solve 100% of the security problem

Protecting Data

- Determine default amount of access:
  - Goal is typically to configure as “deny by default,” also known as “least privilege” access.
  - This approach means only specifically authorized users may access the object.
  - The is the literal opposite of how most systems are configured.
- Decisions may be driven by regulatory compliance mandates, legal requirements, or best practices.

WARNING: The default IBM i authority is shipped preset to *CHANGE

Get Authority to Access an Object

To access or use an object, a user must have sufficient authority to the object. Authority can come from:

01 *ALLOBJ special authority

02 Private authority (explicit authority to the object)

03 *PUBLIC authority (default authority for the object)

04 Adopted authority (programming ‘trick’ for gifting temporary authority via the approved application)

helpsystems

Authority Shortcuts

IBM i contains 4 pre-defined authority templates …

	*OBJOPR	*OBJMGT	*OBJEXIST	*OBJALTER	***OBJREF**	*READ	*ADD	*UPD	*DLT	***EXECUTE**
*ALL	X	X	X	X	X	X	X	X	X	X
*CHANGE	X					X	X	X	X	X
*USE	X					X				X
*EXCLUDE										

helpsystems

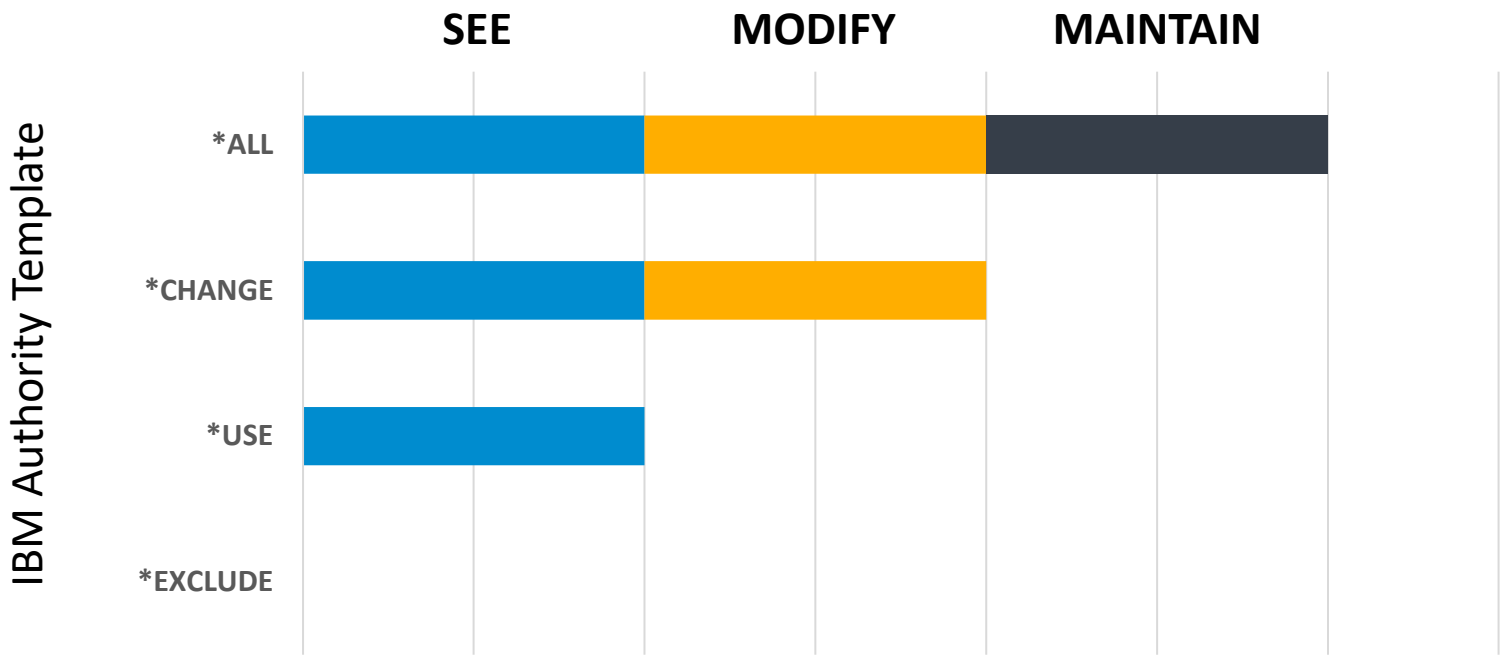
Authority Shortcuts

… to more quickly & easily assign complex combinations of authority permissions

	*OBJOPR	*OBJMGT	*OBJEXIST	*OBJALTER	***OBJREF**	*READ	*ADD	*UPD	*DLT	***EXECUTE**
*ALL	X	X	X	X	X	X	X	X	X	X
*CHANGE	X					X	X	X	X	X
*USE	X					X				X
*EXCLUDE										

helpsystems

OLS Authority Templates



Authority Shortcuts

Although endless combinations are possible, these templates help keep things simple.

***EXCLUDE**	Object cannot be accessed (unless user has *ALLOBJ).
***USE**	Minimum authority necessary to “use” the object in any way. (read it / run it / look within it).
***CHANGE**	Adds the ability to modify the object’s contents.
***ALL**	Can do everything, including deleting the object! Do NOT grant lightly; however, it is more granular than *ALLOBJ.

Deploy using the IBM i templates whenever possible.

Authority Shortcuts

These are the **OBJECT** authorities.

	*OBJOPR	*OBJMGT	*OBJEXIST	*OBJALTER	*OBJREF	*READ	*ADD	*UPD	*DLT	*EXECUTE
*ALL	X	X	X	X	X	X	X	X	X	X
*CHANGE	X					X	X	X	X	X
*USE	X					X				X
*EXCLUDE										

helpsystems

Authority Shortcuts

*OBJOPR – Object Operational	Look at the description of an object and use the object as determined by the data authorities the user has.
*OBJMGT – Object Management	Move or rename an object or add members to database files. Superset of *OBJALTER and *OBJREF
*OBJEXIST – Object Existence	Change ownership and delete the object, free storage for the object, perform save and restore operations
*OBJALTER – Object Alter	Add, clear, initialize and reorganize members of database files, after and add attributes of database files, add and remove triggers, change attributes of SQL packages
*OBJREF – Object Reference	Specify database file as the parent in a referential constraint
*AUTLMGT – Authorization List Management	Add and remove users and their authorities from an authorization list.

Authority Shortcuts

And these are the **DATA** authorities.

	*OBJOPR	*OBJMGT	*OBJEXIST	*OBJALTER	***OBJREF**	*READ	*ADD	*UPD	*DLT	***EXECUTE**
*ALL	X	X	X	X	X	X	X	X	X	X
*CHANGE	X					X	X	X	X	X
*USE	X					X				X
*EXCLUDE										

helpsystems

Authority Shortcuts

*READ	Display the contents of an object, such as viewing the records in a file
*ADD	Add entries to an object, such as adding messages to a message queue, or records to a file
*UPD (Update)	Change entries in an object, such as changing records in a file
*DLT (Delete)	Remove entries from an object, such as removing messages from a message queue or deleting records from a file
*EXECUTE	Run a program or search a library or directory

helpsystems

Inclusive OR

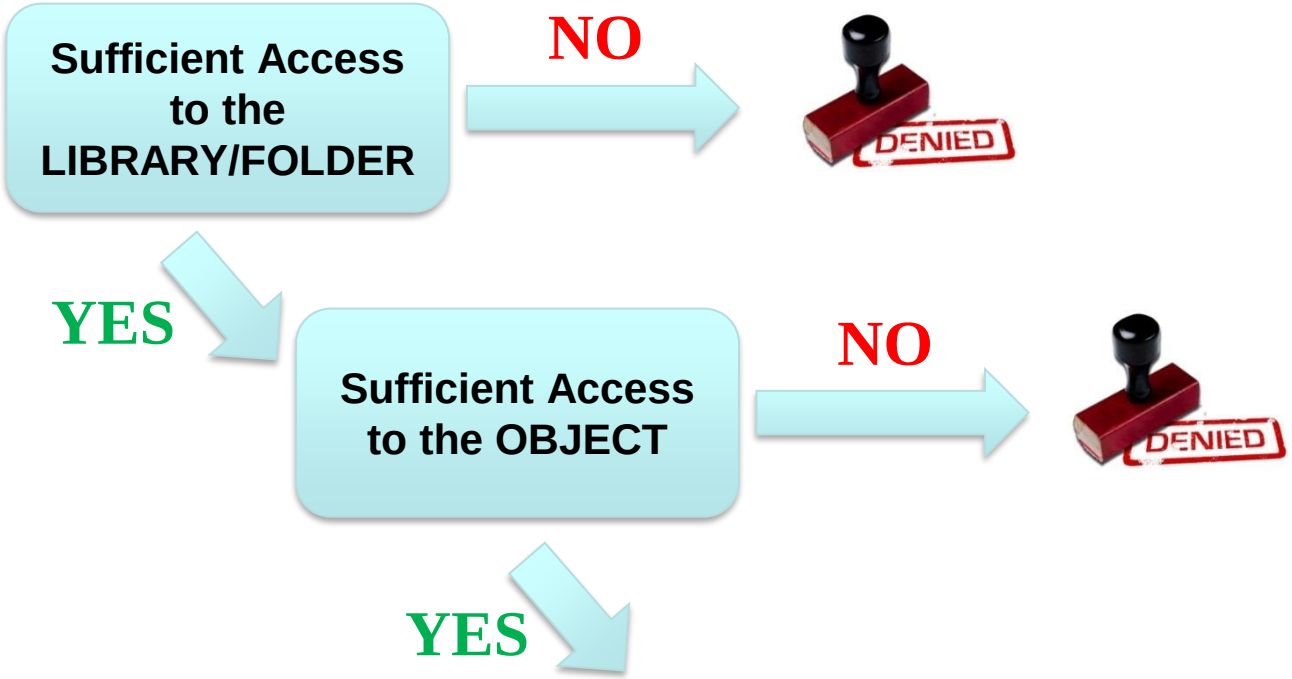
What about conflicting authorities assigned to multiple Group Profiles?

	*OBJOPR	*OBJMGT	*OBJEXIST	*OBJALTER	***OBJREF**	*READ	*ADD	*UPD	*DLT	***EXECUTE**
Group A → *ALL	X	X	X	X	X	X	X	X	X	X
Group B → *EXCLUDE										
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Result → *ALL	X	X	X	X	X	X	X	X	X	X

helpsystems

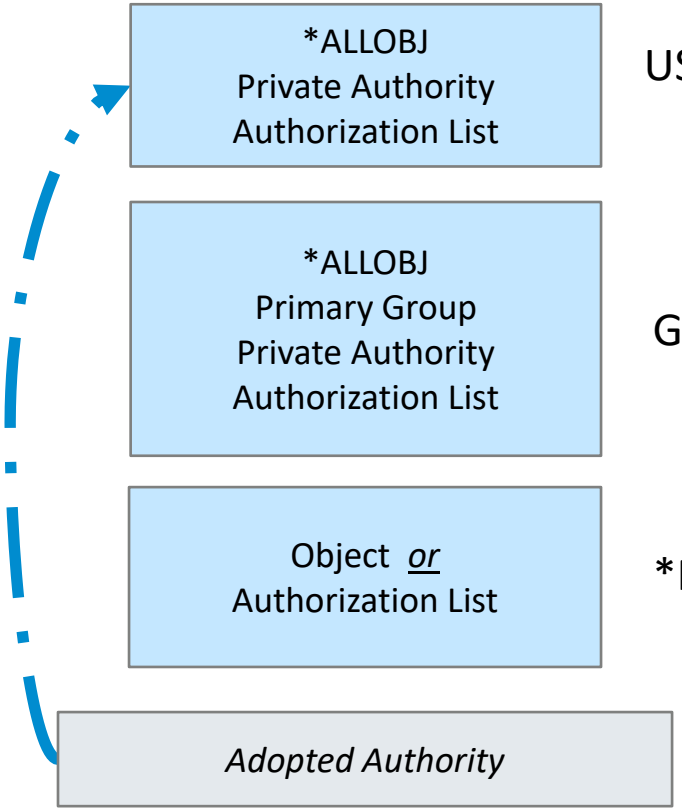
Authority Considerations

IBM i performs TWO primary evaluations before permitting access to an object.



helpsystems

Authority Search Order



USER

GROUP(S)

*PUBLIC

Authority checking stops when *ANY* applicable authority directive is found – sufficient or not

Repeats for each group profile until sufficient authority is accumulated or no more groups are left to process

Used only when no private authority is found for the individual user or their group(s)

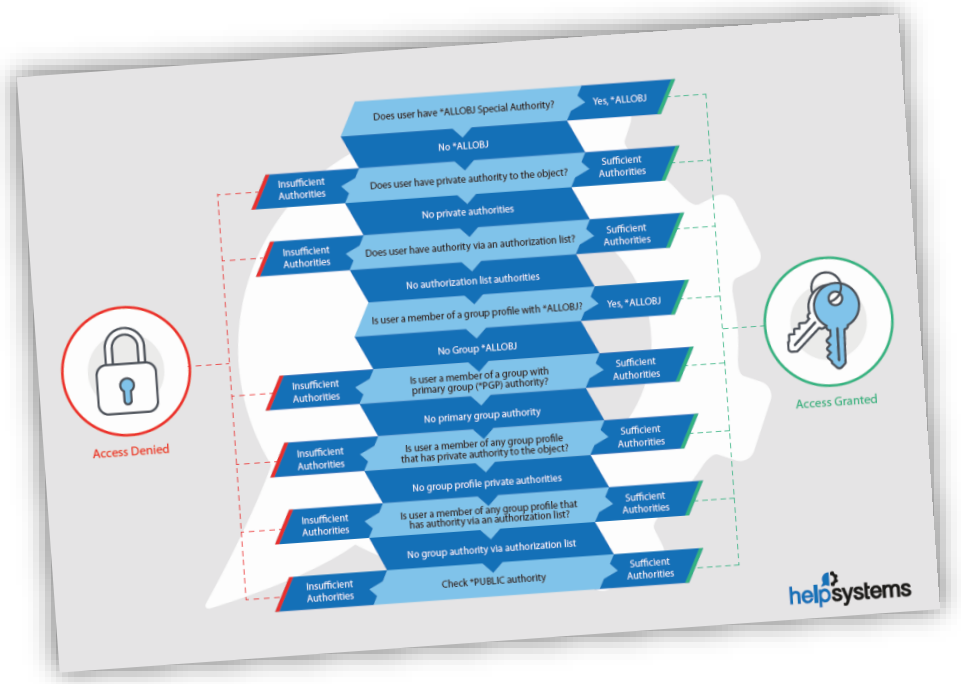
Checks program owner's authority if user authority is not sufficient. This is an optional step performed as one last chance before a "not authorized" message is issued

helpsystems

Authority Search Order

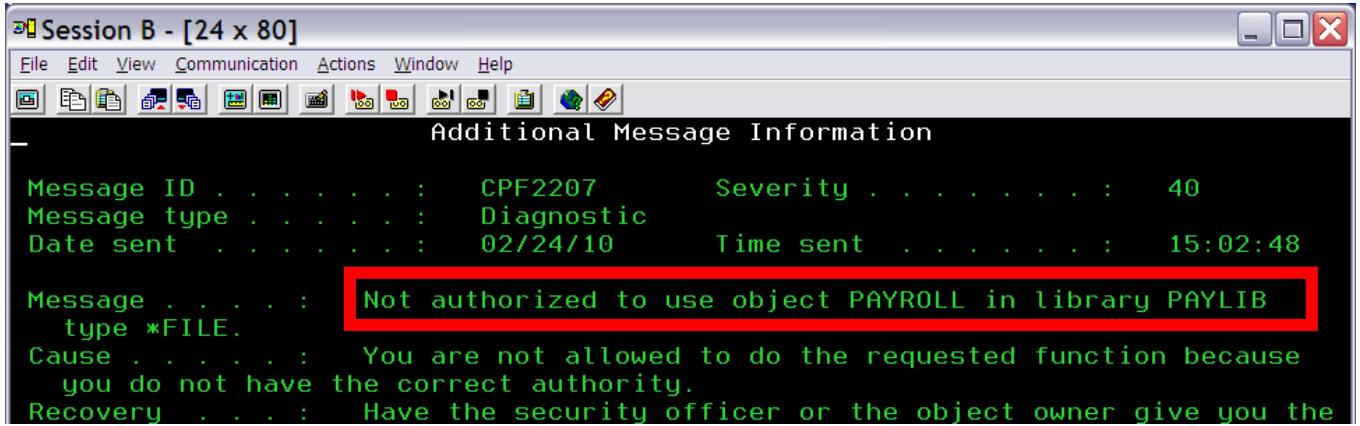
Want a Copy?

Robin.Tatam@HelpSystems.com



Authority Considerations

If (ok, *when*) you over-secure an object, or fail to elevate authority at runtime, the user will receive an authority failure message. An “AF” entry will also be logged to the QAUDJRN audit journal if system event auditing is active (as it should be!)



helpsystems

Authority Considerations

Do NOT respond to authority errors by granting the user *ALLOBJ special authority as this is a system-wide override! Determine *why* the failure occurred and correct it.

*ALLOBJ Special Authority

- *ALLOBJ is a special (admin) privilege assigned within the user profile. It – along with all special authorities – are also inherited from a user's group(s).
- Provides the ability to access **EVERY** object on the system. In effect, providing *ALL authority to every object on the system, including within the OS itself!
- You **cannot** prevent an *ALLOBJ user from accessing an object.
- Having *ALLOBJ can often facilitate obtaining the other 7 special authorities.

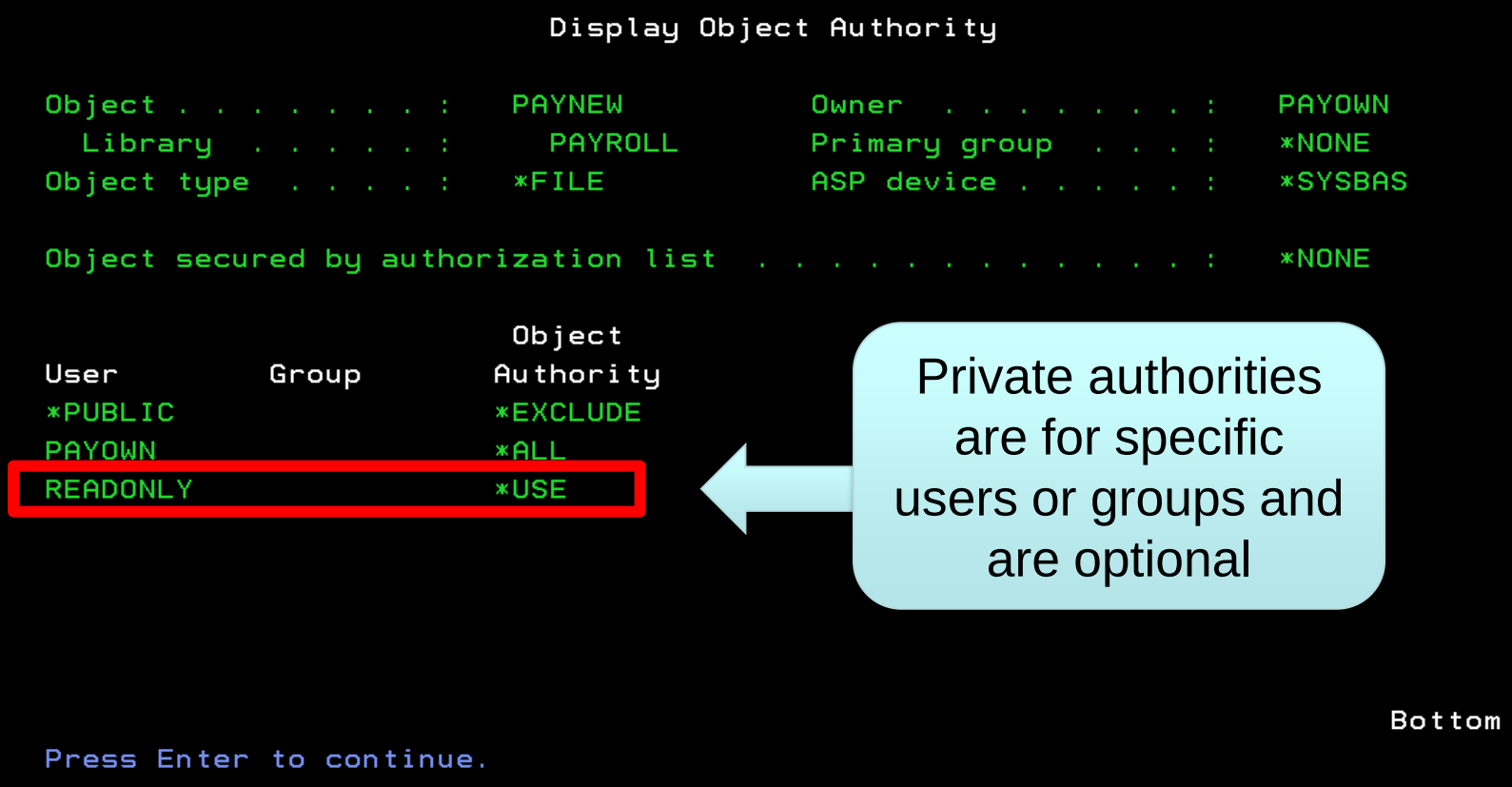
Private Authority

Private authority is “**named**” access, and is granted to an individual user or group profile. (in contrast, public authority represents “**default**” access).

Private authority can be more restrictive but is typically less restrictive than public authority.

Common terms: **deny-by-default** & **least privilege**

helpsystems


Display Object Authority
Object . . . . . : PAYNEW
Library . . . . . : PAYROLL
Object type . . . . : *FILE
Owner . . . . . : PAYOWN
Primary group . . . : *NONE
ASP device . . . . . : *SYSBAS
Object secured by authorization list . . . . . : *NONE
User
Group
Object Authority
*PUBLIC *EXCLUDE
PAYOWN *ALL
READONLY *USE
Private authorities are for specific users or groups and are optional
Bottom
Press Enter to continue.
F3=Exit F11=Display detail object authorities F12=Cancel F17=Top
F18=Bottom
(C) COPYRIGHT IBM CORP. 1980, 2005.

Assigning Private Authority

To give private authority, use the **GRTOBJAUT, EDTOBJAUT,** and **CHGAUT** commands.

GRTOBJAUT OBJ(AR_LIB/RCVFILE) OBJTYPE(*FILE) USER(ROBIN) AUT(*USE)

Robin can view the contents of the file - *USE

To remove existing authority, use the **RVKOBJAUT, EDTOBJAUT,** and **CHGAUT** commands.

*RVKOBJAUT OBJ(AR_LIB/RCVFILE) OBJTYPE(*FILE) USER(ROBIN) AUT(*ALL)*

Removes whatever authority Robin has to the file

Public Authority

IBM i contains a unique concept called Public Authority which is the *default* permission granted to a user who has not been granted any private (aka named) authority.

Public authority is determined by:

- For native objects:
  - public authority is assigned starting from the CRTxxx command
- For IFS objects:
  - public authority is inherited from the parent directory

helpsystems

Public Authority

For native objects, IBM resolves the public authority setting from the create command to the library description to the QCRTAUT system value.

Once *PUBLIC authority is resolved, it's permanent—there is no ongoing dynamic link.

helpsystems

Public Authority

There is nothing technically wrong with the *concept* of default public authority.

Problems occur when the QCRTAUT system value remains at its shipped value of *CHANGE

(Because that's sufficient to read, change, and delete the data!)

helpsystems

Public Authority

I recommend establish a *PUBLIC authority default for each individual library.

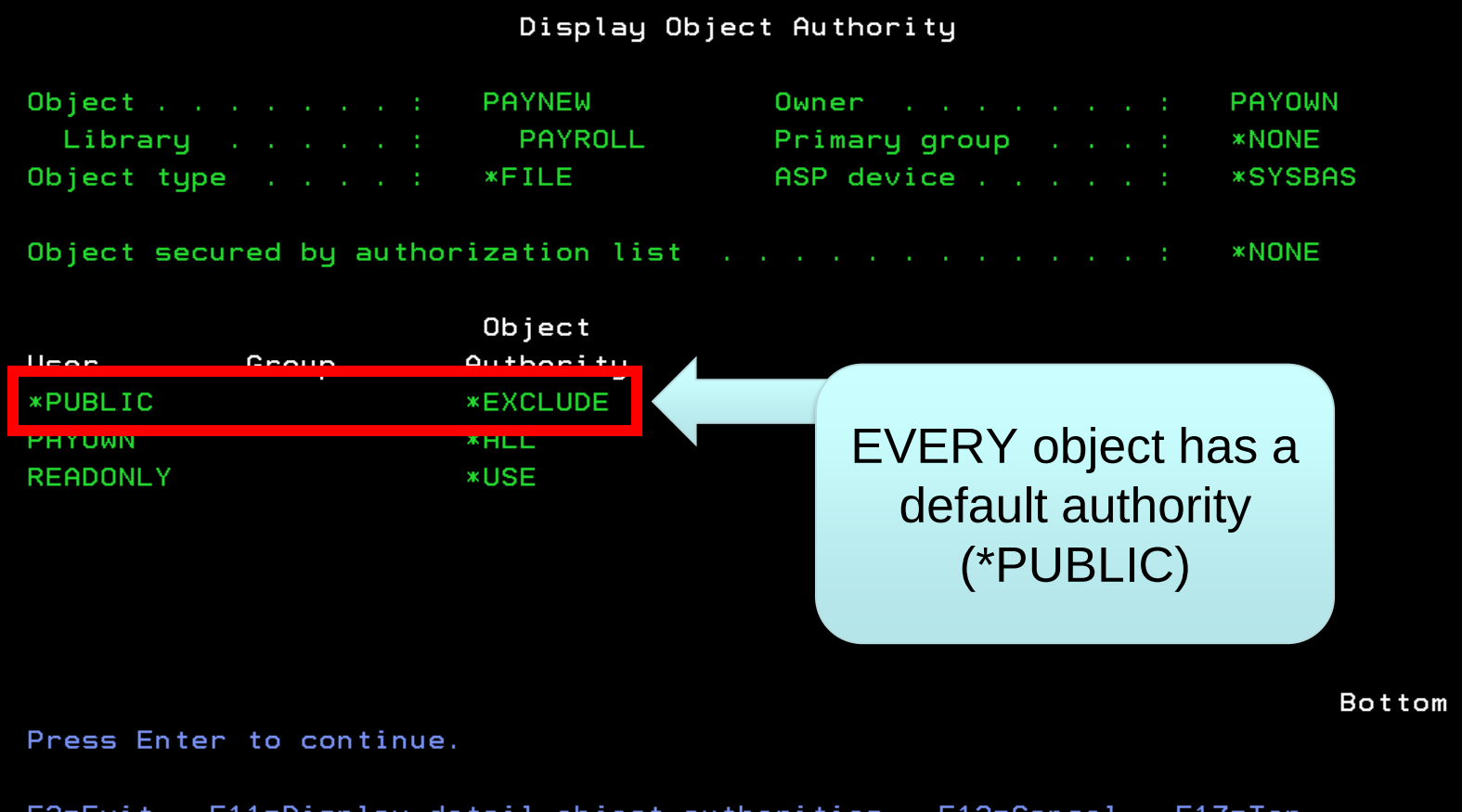
CRTxxx
AUT(*LIBCRTAUT)

DSPLIBD
CRTAUT(*EXCLUDE)

DSPSYSVAL
QCRTAUT

This permits granular control. It's very useful when the server hosts multiple applications with varying authority requirements.

helpsystems


Display Object Authority
Object . . . . . : PAYNEW
Owner . . . . . : PAYOWN
Library . . . . . : PAYROLL
Primary group . . . : *NONE
Object type . . . . : *FILE
ASP device . . . . . : *SYSBAS
Object secured by authorization list . . . . . : *NONE
Object
*PUBLIC *EXCLUDE
PAYOWN *ALL
READONLY *USE
EVERY object has a default authority (*PUBLIC)
Bottom
Press Enter to continue.
F3=Exit F11=Display detail object authorities F12=Cancel F17=Top
F18=Bottom
(C) COPYRIGHT IBM CORP. 1980, 2005.

Authorization Lists

Authorization lists are an **organizational mechanism** for securing *objects* with similar security requirements:

- All objects secured by an authorization list obtain private authorities (and, optionally, public authorities) from the list
- You can still grant specific authorities to objects to augment (override) the authorities on the authorization list

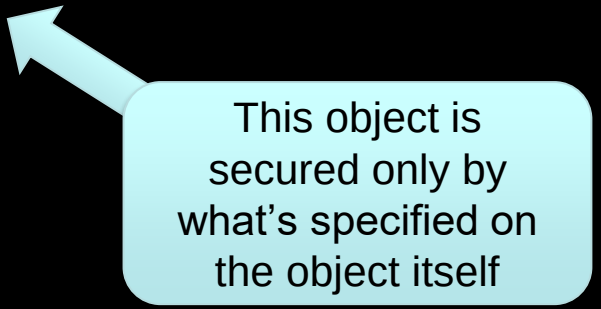
CRTAUTL AUTL(myautl) AUT(*EXCLUDE)

Then use ADDAUTLE or EDTAUTL to maintain the list entries

24x7 shop? Changing authorities on an authorization list does NOT require a lock on the object.

Display Object Authority

```
Object . . . . . :   PAYNEW          Owner . . . . . :   PAYOWN
  Library  . . . . :     PAYROLL     Primary group . . . :   *NONE
Object type  . . . . :   *FILE       ASP device . . . . . :   *SYSBAS

Object secured by authorization list  . . . . . . . . . . . . :   *NONE

                          Object
User         Group        Authority
*PUBLIC                   *EXCLUDE
PAYOWN                    *ALL
READONLY                  *USE
```



Bottom

Press Enter to continue.

F3=Exit F11=Display detail object authorities F12=Cancel F17=Top
F18=Bottom

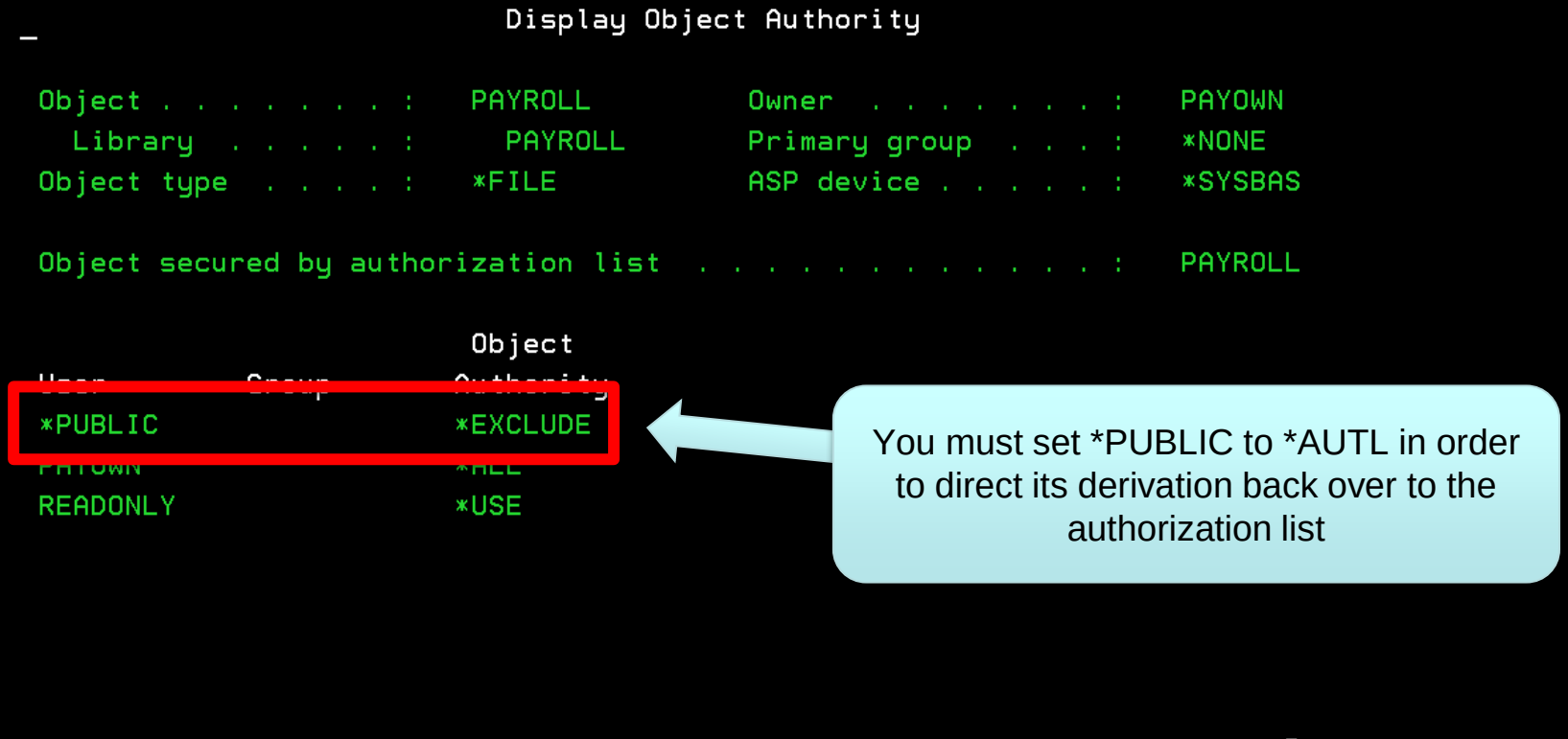
(C) COPYRIGHT IBM CORP. 1980, 2005.

```
                          Display Object Authority

Object . . . . . :   PAYROLL          Owner  . . . . . :   PAYOWN
  Library  . . . . :     PAYROLL      Primary group  . . :   *NONE
Object type  . . . :   *FILE          ASP device . . . . :   *SYSBAS

Object secured by authorization list  . . . . . . . . . . . . :   PAYROLL

                          Object
User         Group        Authority
*PUBLIC                   *EXCLUDE
PAYOWN                    *ALL
READONLY                  *USE

                                                                  Bottom
Press Enter to continue.

F3=Exit   F11=Display detail object authorities   F12=Cancel
F14=Display authorization list   F17=Top         F18=Bottom
(C) COPYRIGHT IBM CORP. 1980, 2005.
```

This object is additionally secured by the PAYROLL authorization list

```
                          Display Object Authority

Object . . . . . :   PAYROLL          Owner  . . . . . :   PAYOWN
  Library  . . . . :     PAYROLL      Primary group  . . :   *NONE
Object type  . . . :   *FILE          ASP device . . . . :   *SYSBAS

Object secured by authorization list  . . . . . . . . . . . . :   PAYROLL

                                      Object
User          Group                   Authority
*PUBLIC                               *EXCLUDE
PAYOWN                                *ALL
READONLY                              *USE

                                                                  Bottom
Press Enter to continue.

F3=Exit   F11=Display detail object authorities   F12=Cancel
F14=Display authorization list   F17=Top          F18=Bottom
(C) COPYRIGHT IBM CORP. 1980, 2005.
```

These authorities take precedence over those on the authorization list


Display Object Authority
Object . . . . . : PAYROLL
Owner . . . . . : PAYOWN
Library . . . . . : PAYROLL
Primary group . . . : *NONE
Object type . . . . . : *FILE
ASP device . . . . . : *SYSBAS
Object secured by authorization list . . . . . : PAYROLL
Object
*PUBLIC *EXCLUDE
READONLY *USE
You must set *PUBLIC to *AUTL in order to direct its derivation back over to the authorization list
Bottom
Press Enter to continue.
F3=Exit F11=Display detail object authorities F12=Cancel
F14=Display authorization list F17=Top F18=Bottom
(C) COPYRIGHT IBM CORP. 1980, 2005.

Group Profile or Authorization List?

A popular question!

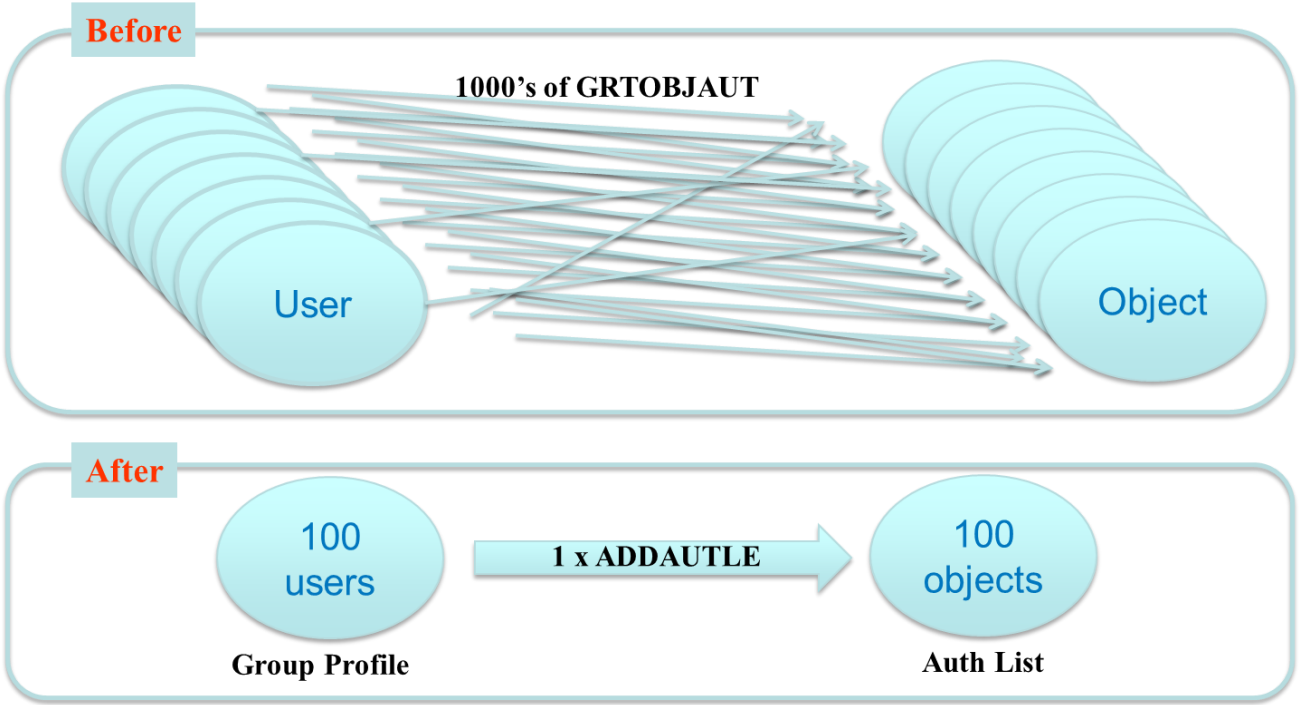
It's typically not a decision of *which* one you should use; consider using them both together.

Remember:

- Group Profiles associate users with similar access requirements.
- Authorization List secures objects with similar security requirements.

helpsystems

Group Profile or Authorization List?



helpsystems

An Alternate Method:

Adopted Authority

Adopted Authority

- Normally, a program executes with the authority of only the user running it.
- Adoption comes into play if the IBM i authority check determines that the user does not have sufficient permission on their own.
- Adoption adds the authority of a programs owner which can (potentially, if the program owner has more authority than the calling user) temporarily increase the effective authority.
- Adopted authority is only in effect while the program runs.

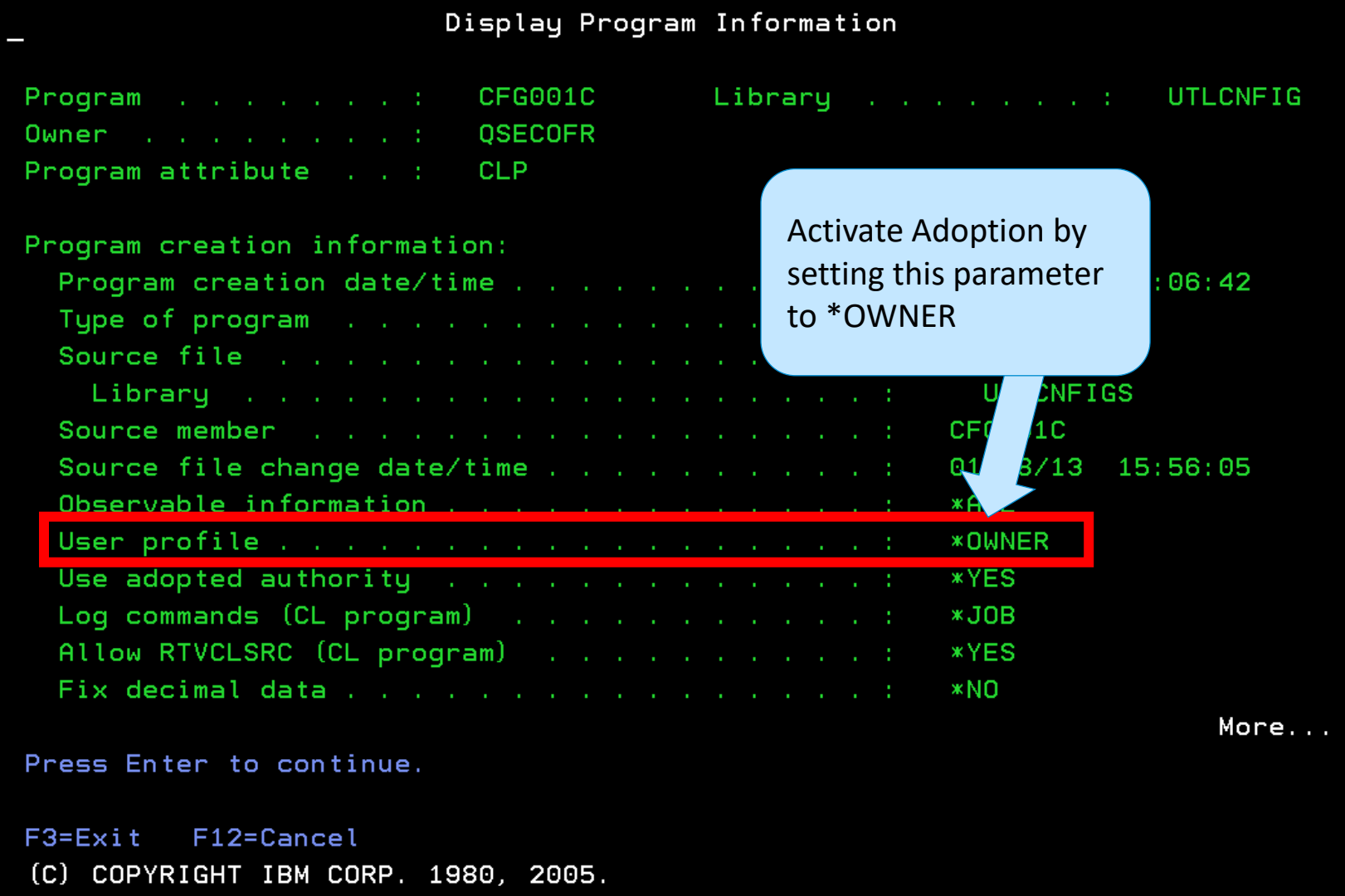
Adopted Authority

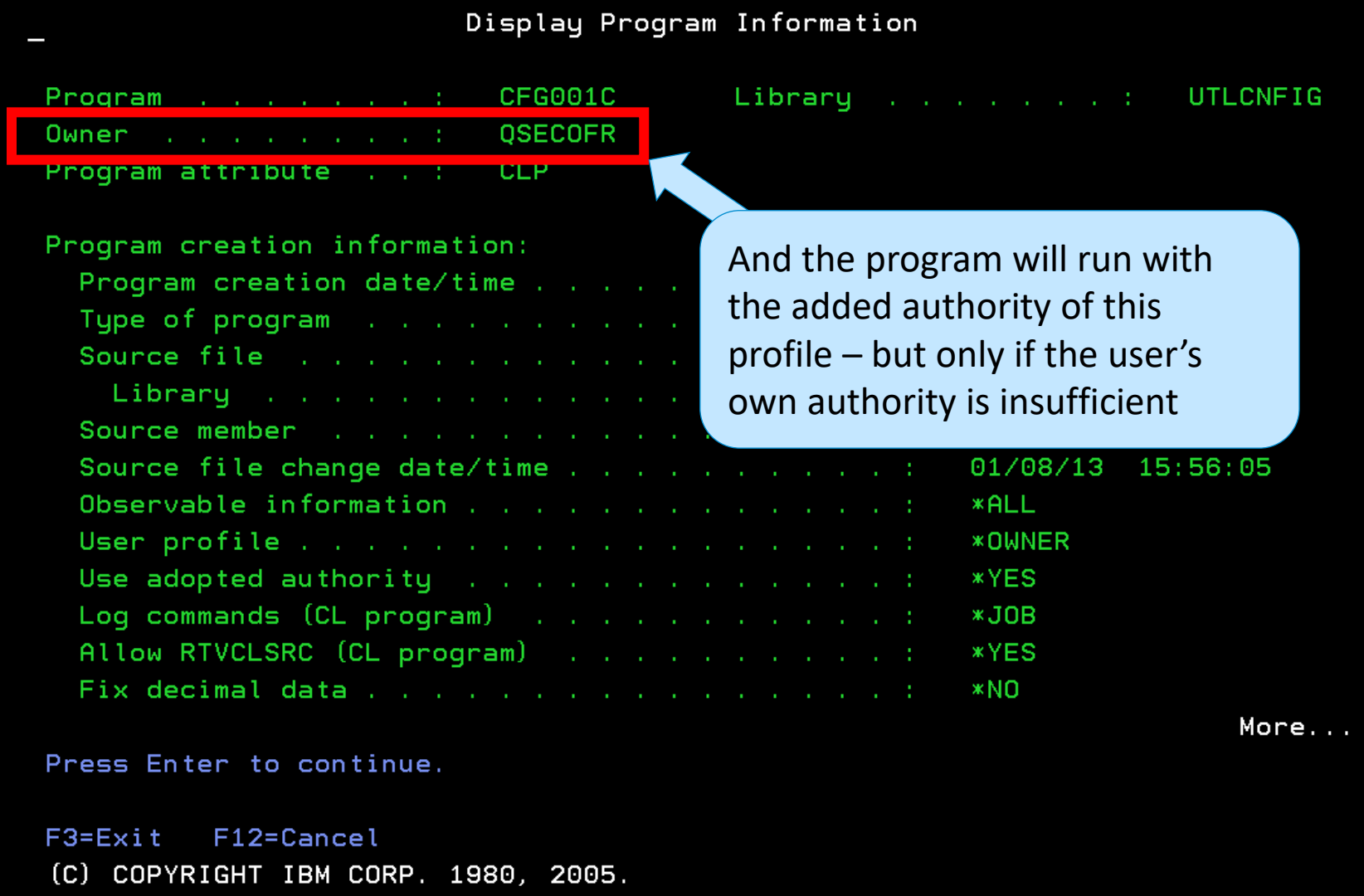
In addition, authority can be inherited from programs higher in the call stack; however, that is a separate attribute on the program object.

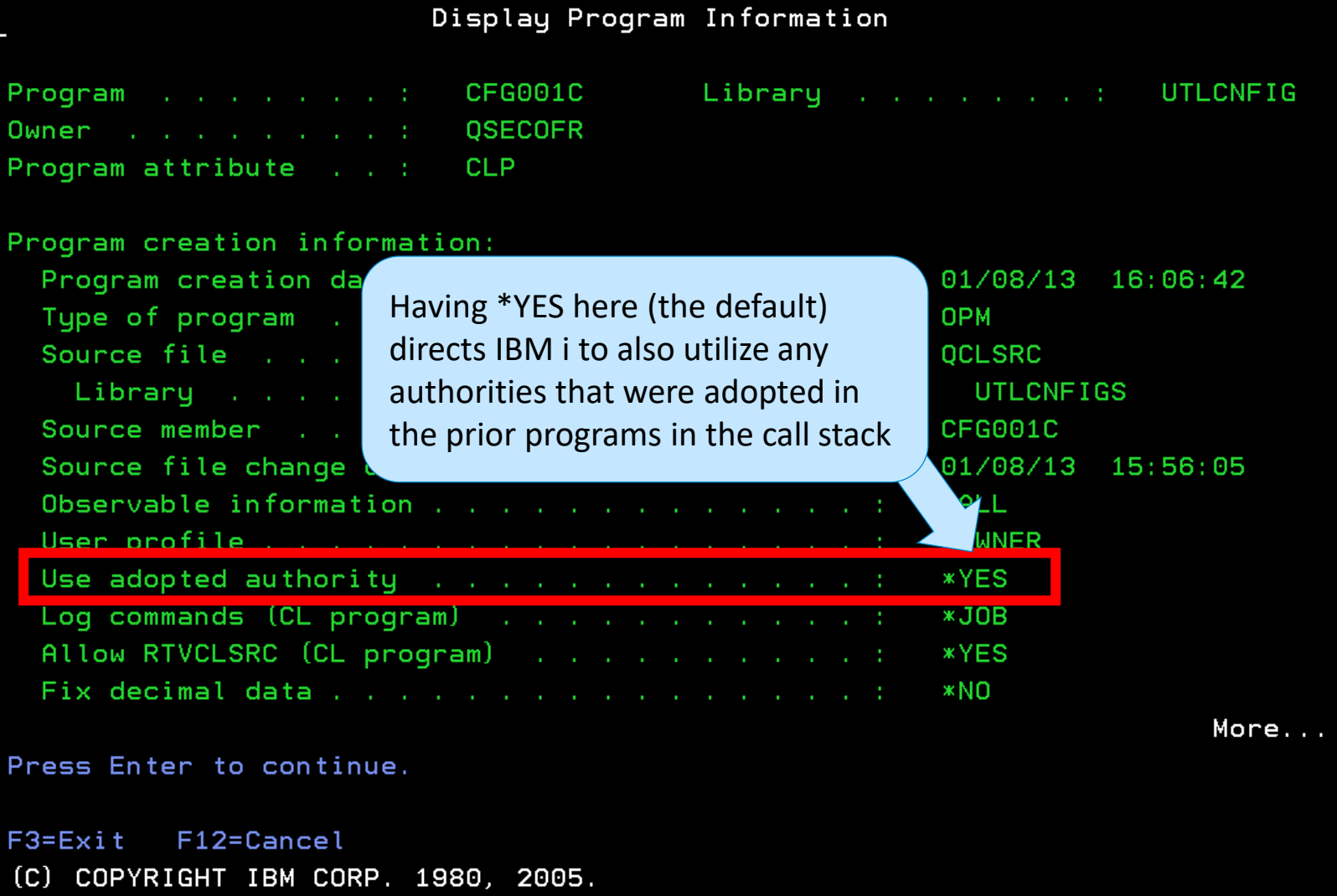
Some adoption nuances:

- Authority is additive to the user (adoption cannot reduce a user's authority)
- Adoption is not observed in the Integrated File System (use a profile swap instead)
- Authority can be adopted from multiple owning profiles if multiple programs.

If a program uses adopted authority, it should never present a command line to the user!

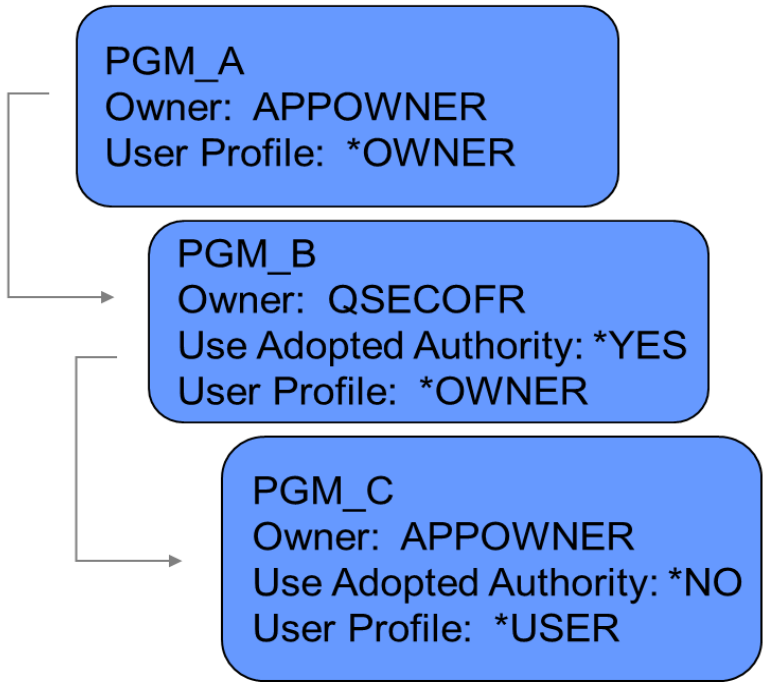

Display Program Information
Program . . . . . : CFG001C
Library . . . . . : UTLCNFIG
Owner . . . . . : QSECOFR
Program attribute . . : CLP
Program creation information:
Program creation date/time . . . . . :06:42
Type of program . . . . . :
Source file . . . . . :
Library . . . . . : CNFIGS
Source member . . . . . : CFG 1C
Source file change date/time . . . . . : 0 3/13 15:56:05
Observable information . . . . . : *A
User profile . . . . . : *OWNER
Use adopted authority . . . . . : *YES
Log commands (CL program) . . . . . : *JOB
Allow RTVCLSRC (CL program) . . . . . : *YES
Fix decimal data . . . . . : *NO
More...
Press Enter to continue.
F3=Exit F12=Cancel
(C) COPYRIGHT IBM CORP. 1980, 2005.
Activate Adoption by setting this parameter to *OWNER


Display Program Information
Program . . . . . : CFG001C
Library . . . . . : UTLCNFIG
Owner . . . . . : QSECOFR
Program attribute . . : CLP
Program creation information:
Program creation date/time . . . .
Type of program . . . . . .
Source file . . . . . .
Library . . . . . .
Source member . . . . . .
Source file change date/time . . . . . : 01/08/13 15:56:05
Observable information . . . . . : *ALL
User profile . . . . . : *OWNER
Use adopted authority . . . . . : *YES
Log commands (CL program) . . . . . : *JOB
Allow RTVCLSRC (CL program) . . . . . : *YES
Fix decimal data . . . . . : *NO
More...
Press Enter to continue.
F3=Exit F12=Cancel
(C) COPYRIGHT IBM CORP. 1980, 2005.
And the program will run with the added authority of this profile – but only if the user's own authority is insufficient


Display Program Information
Program . . . . . : CFG001C Library . . . . . : UTLCNFIG
Owner . . . . . : QSECOFR
Program attribute . . : CLP
Program creation information:
Program creation da 01/08/13 16:06:42
Type of program . OPM
Source file . . . QCLSRC
Library . . . . UTLCNFIGS
Source member . . CFG001C
Source file change 01/08/13 15:56:05
Observable information . . . . . : *ALL
User profile . . . . . : *OWNER
Use adopted authority . . . . . : *YES
Log commands (CL program) . . . . . : *JOB
Allow RTVCLSRC (CL program) . . . . . : *YES
Fix decimal data . . . . . : *NO
More...
Press Enter to continue.
F3=Exit F12=Cancel
(C) COPYRIGHT IBM CORP. 1980, 2005.
Having *YES here (the default) directs IBM i to also utilize any authorities that were adopted in the prior programs in the call stack

Adopted Authority

Program Call Stack



Users Checked

user then APPOWNER

user then APPOWNER (from PGM_A) then QSECOFR

Only *user* because USEADPAUT(*NO) and USRPRF(*USER)

helpsystems

Considerations

A few extra items to consider:

- Applications should set newly-created objects to the correct authority and ownership at run time.
- You can’t create new objects in a library with only *USE authority.
- You can’t create new members in files with only *USE authority.
- Secure your application source code.
- Audit access attempts against highly-sensitive objects.
- Activate *AUTFAIL and monitor for “AF” authority failures in QAUDJRN.

Next Steps

Let’s chat about the limitations of Object Level Security

First Step or Last Step?

Object Level Security is the ‘Gold Standard’ of Security on IBM i

Often easier than people think

Is respected by all access methods

Definitive in an audit

Tools to help as of v7.3

Not the easiest concept to grasp

Not flexible to different interfaces

Other options may be quicker to implement

Doesn’t solve 100% of the security problem

i = integrated!

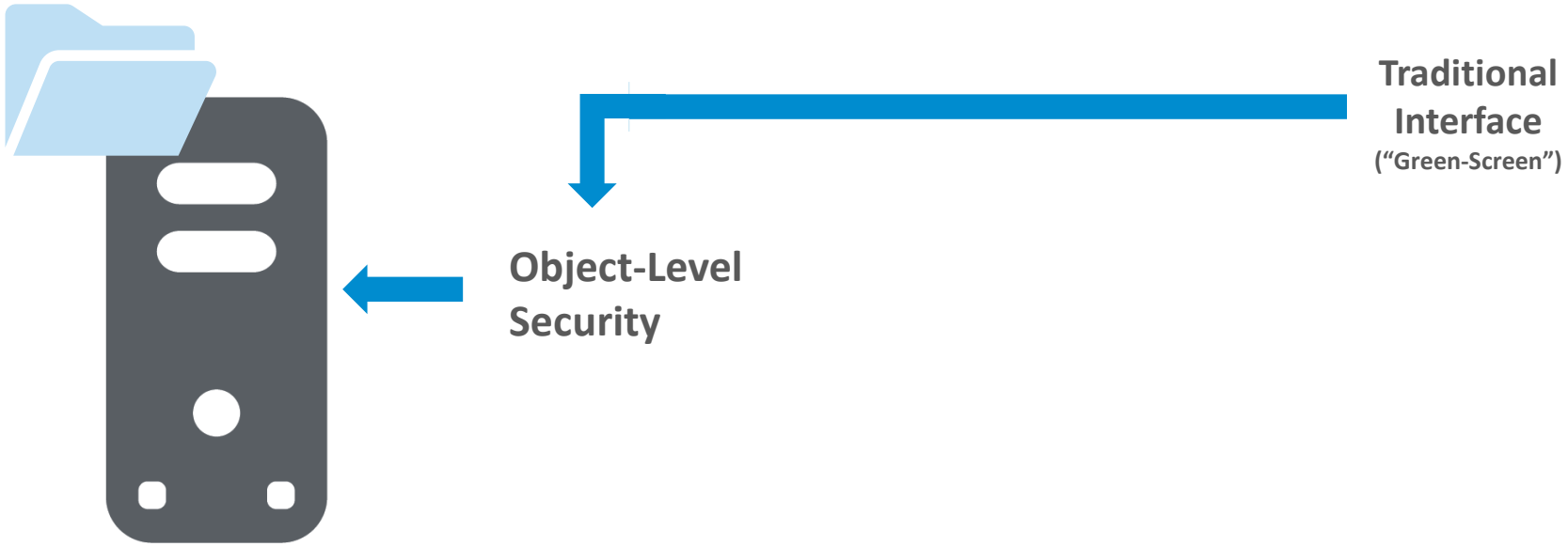
Everything within IBM i has been deeply integrated, including the famous **Db2 database**.

A person who has knowledge of profile credentials can attempt to access the database through every interface now supported by the modern Power Systems server.

Object Level Security Works Everywhere

Green Screen
Application WUI or GUI
Java
Navigator
And the list goes on …

Object Level Security in Visual Terms



Get Authority to Access an Object

To access or use an object, a user must have sufficient authority to the object. Authority can come from:

01 *ALLOBJ special authority

02 Private authority (explicit authority to the object)

03 *PUBLIC authority (default authority for the object)

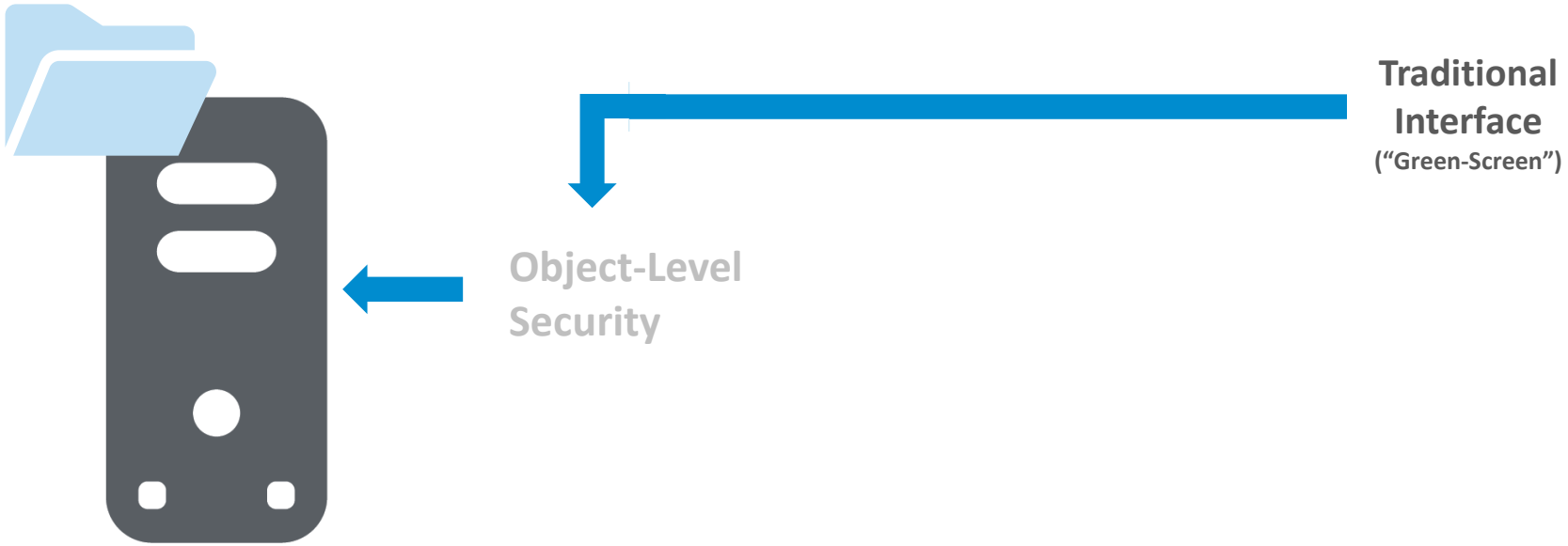
04 Adopted authority (programming ‘trick’ for gifting temporary authority via the approved application)

helpsystems

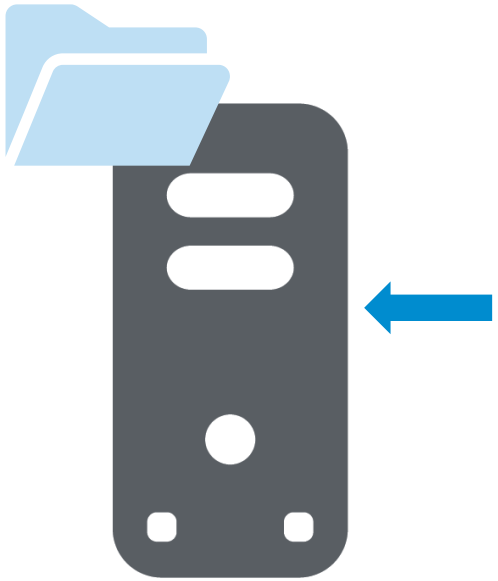
Will Access Be Granted?

- In calendar 2021, each IBM i system we audited had:
  - An average of **244 profiles** with *ALLOBJ (“root”) privileges
  - An average of **286 profiles** with non-limited capabilities (aka command line permission)
  - Less than **8%** of application libraries set to *PUBLIC(*EXCLUDE) (deny by default)
  - **73%** had no exit programs to monitor their TCP/IP interface activity

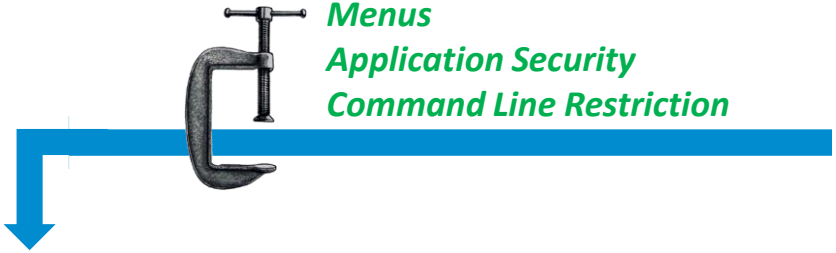
Weak OLS? Compensating Controls Are Necessary



Many Of Which Are Already In Use



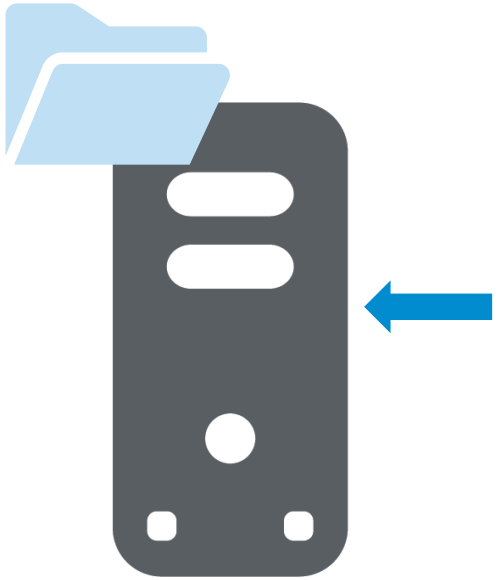
Object-Level Security



Menus
Application Security
Command Line Restriction

Traditional Interface
("Green-Screen")

But What About Non-Traditional?



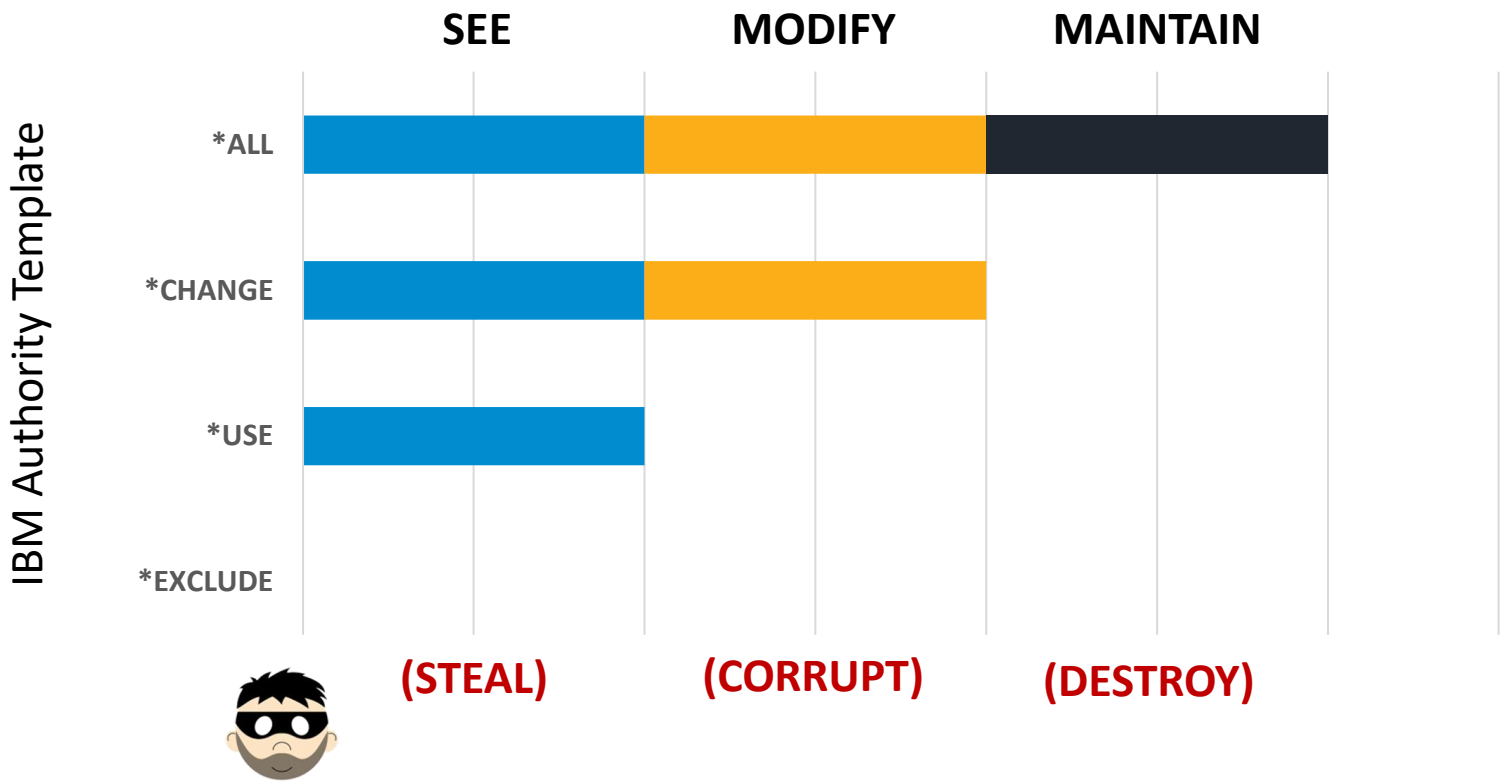
Menus
Application Security
Command Line Restriction

Traditional Interface
(“Green-Screen”)

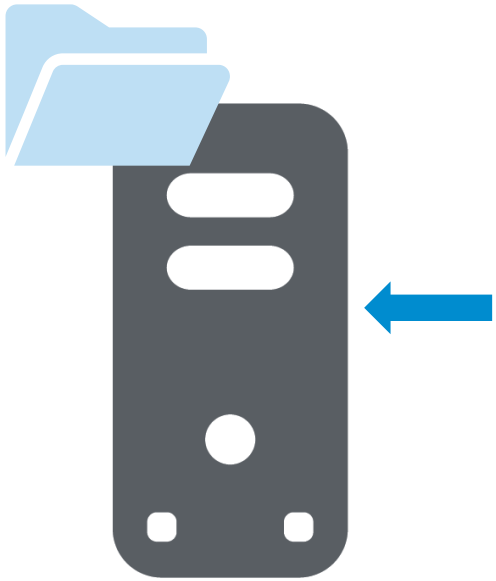
Object-Level Security

Non-Traditional Interfaces
(ODBC/JDBC, FTP, DDM, IFS Drive share)

OLS Authority Templates



Compensating Controls Are Necessary On Both Sides



Menus
Application Security
Command Line Restriction

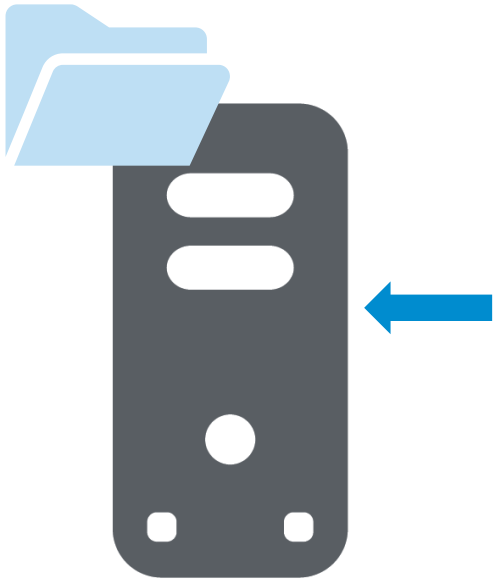
Traditional Interface
(“Green-Screen”)

Object-Level Security

Exit Programs

Non-Traditional Interfaces
(ODBC/JDBC, FTP, DDM, IFS Drive share)

OLS Rules Supreme!



Traditional Interface
("Green-Screen")

Object-Level Security

Non-Traditional Interfaces
(ODBC/JDBC, FTP, DDM, IFS Drive share)

But Remember …

Object Level Security

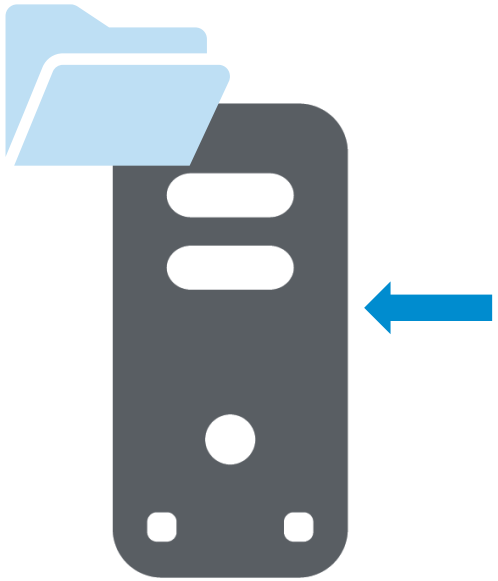
is “One Size Fits All”

But Remember …

Most data isn't as secure as the owner thinks, but even if it is:

1. Authority for applications carries through to all user interfaces.
2. IBM i does NOT differentiate between different access methods.
3. Adequate auditing of network-initiated requests is not available.
4. Command line permissions can still be circumvented.

OLS + Compensating Controls = Ideal



Menus
Application Security
Command Line Restriction

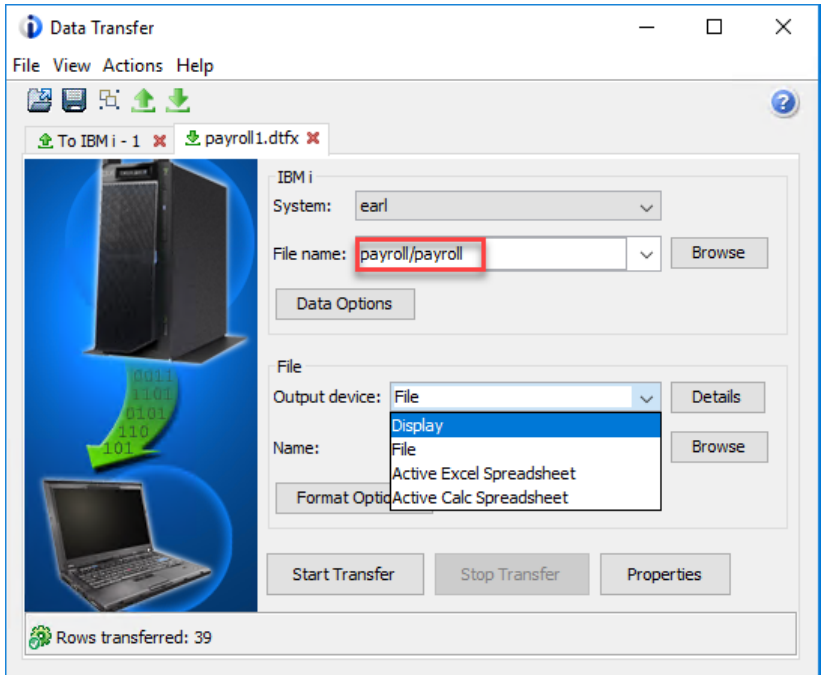
Traditional Interface
("Green-Screen")

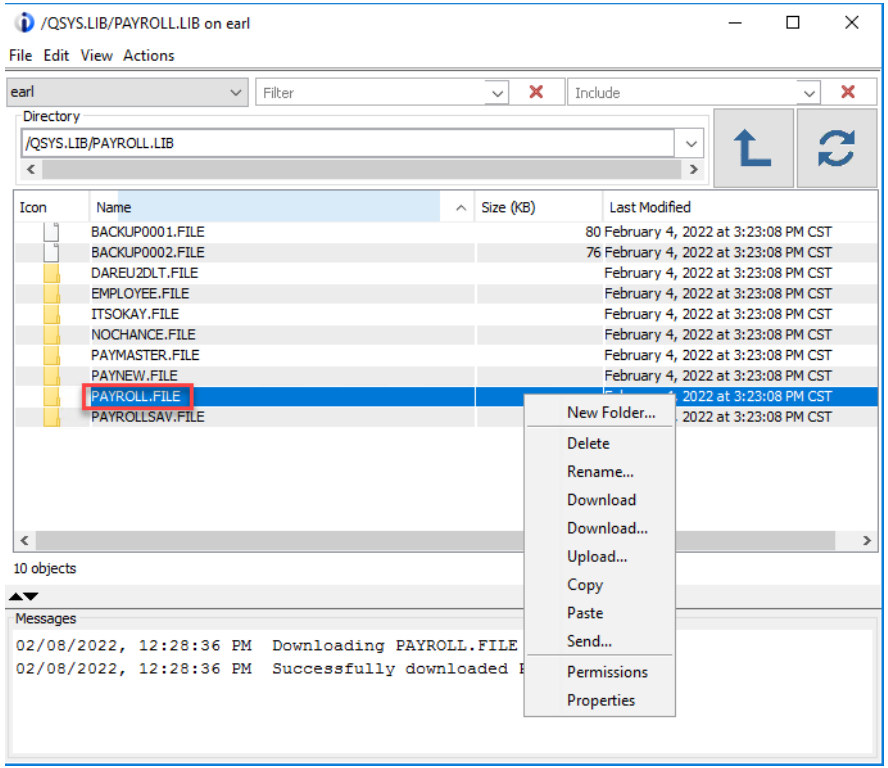
Object-Level Security

Exit Programs

Non-Traditional Interfaces
(ODBC/JDBC, FTP, DDM, IFS Drive share)

Alternative Ways to See Data





helpsystems

Alternative Ways to See Data

Administrator: Command Prompt

```
C:\Users\Administrator>ftp earl
Connected to earl.example.com.
220-QTCP at earl.example.com.
220 Connection will close if idle more than 5 minutes.
501 OPTS unsuccessful; specified subcommand not recognized.
User (earl.example.com:(none)): sandi
331 Enter password.
Password:
230 SANDI logged on.
ftp> bin
200 Representation type is binary IMAGE.
ftp> get payroll/payroll
200 PORT subcommand request successful.
150 Retrieving member PAYROLL in file PAYROLL in library PAYROLL.
226 File transfer completed successfully.
ftp: 2262 bytes received in 0.10Seconds 21.75Kbytes/sec.
ftp> quit
221 QUIT subcommand received.
```

Untitled* - Run SQL Scripts - earl(Ibmi74)

File Edit Search View Connection Run Explain Monitor Tools Help

```
1 select * from payroll.payroll
```

EMPLOYEE	SSN	SALARY	DEPT
Yul B. Allwright	484152668	89000	EXECUTIVE
Upton O. Goode	484152668	55000	SALES
Hedda Hare	484152668	29000	WAREHOUSE
Lynn C. Doyle	484152668	26000	IT
Lori Driver	484152668	45750	SALES
Maurice Less	484152668	21500	QA
Harry Chin	484152668	47000	IT
Chris P. Bacon	484152668	49000	WAREHOUSE
Krystal Ball	484152668	55000	OPERATIONS
Jed I. Night	484152668	44000	ORDERENTRY
Hugh Murrus	484152668	26000	WAREHOUSE
Hugh Manatee	484230041	62000	SALES
Helen Back	484193221	45000	OPERATIONS
Helena Hanbaskett	436121443	87000	SALES

Done: 39 rows retrieved.

Messages Environment select * from payroll.payroll

02/08/2022, 11:45:10 AM

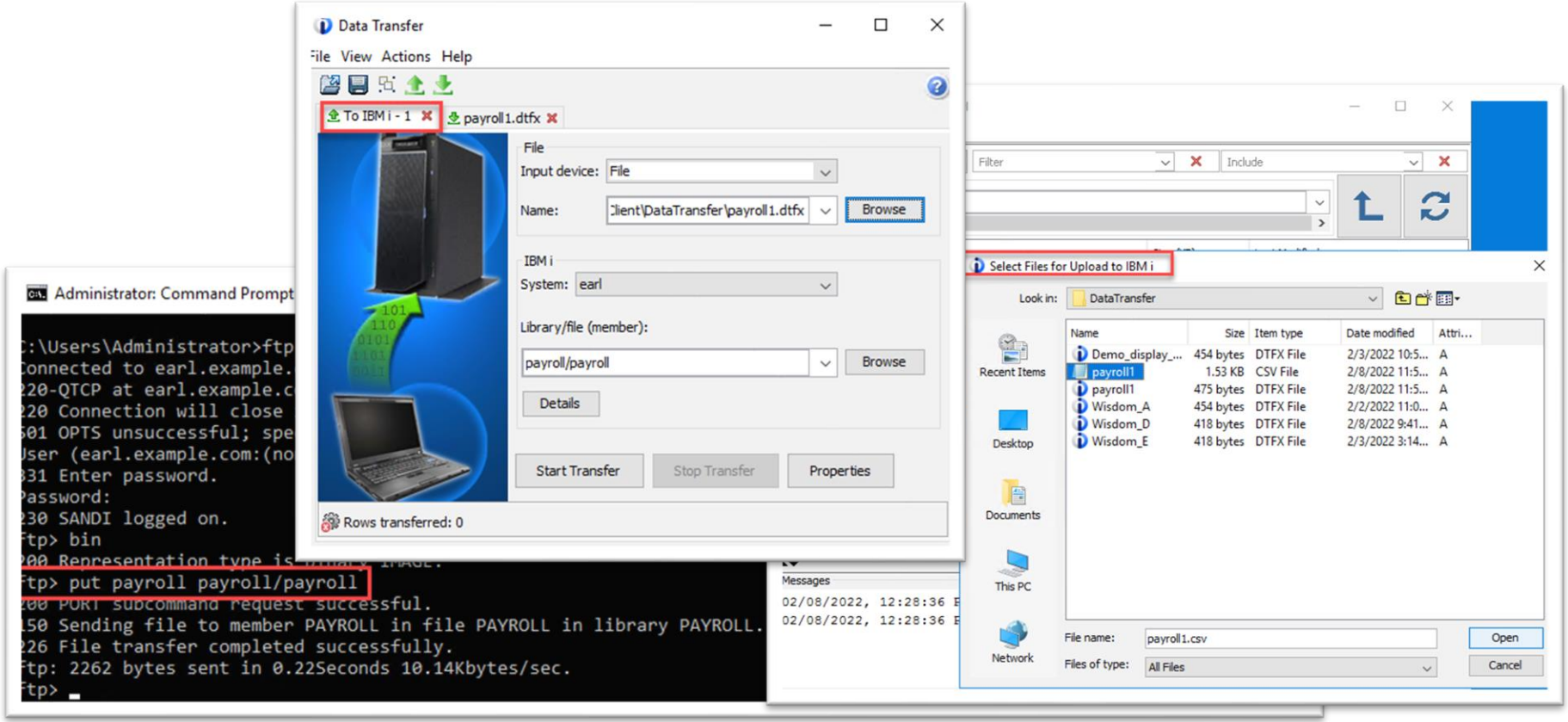
Details...
Columns...
Column Headings
Refresh
Save Results...
Upload Results...
Copy Ctrl+C
Select All Ctrl+A
Print...

Connected to relational database Ibmi74 on earl as SANDI - 084769/QUSER/QZDASOINIT using JDBC configuration 'Default'.

Lines: 1 Ln: 1 Col: 30

helpsystems

Alternative Ways to Modify Data and Objects



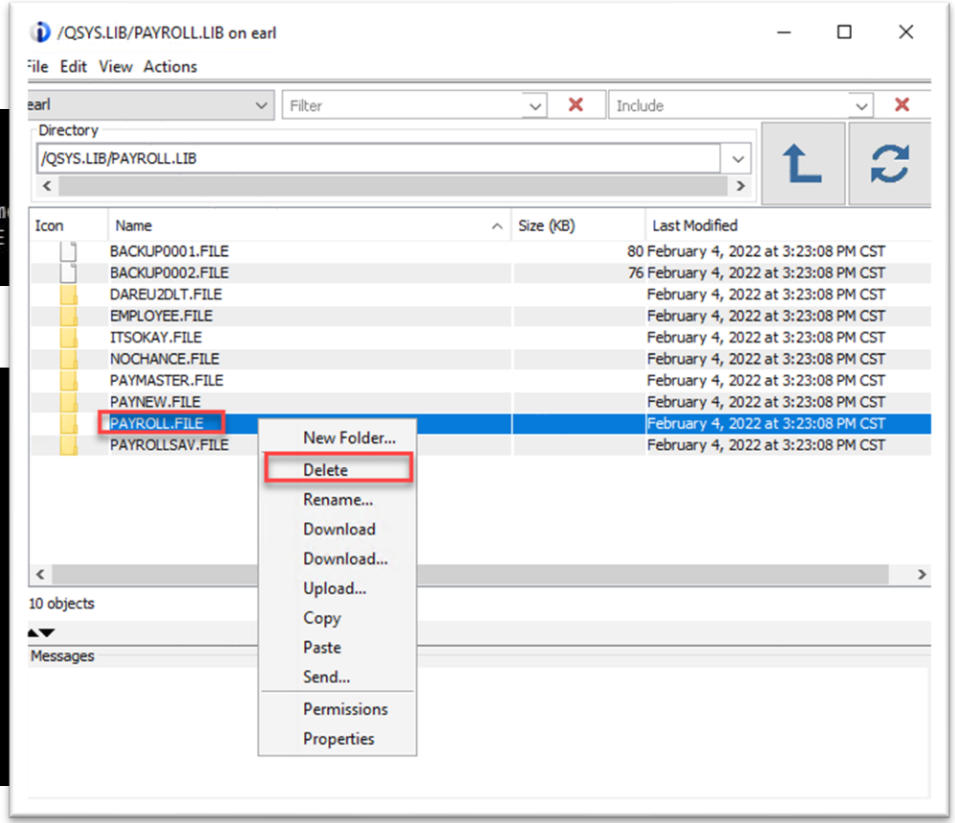
helpsystems

Alternative Ways to “Maintain” Objects

```
ftp> bin
200 Representation type is binary IMAGE.
ftp> rename payroll/payroll2 payroll/payraise
350 RNFR file PAYROLL2 in library PAYROLL accepted. Type new nam
250 File PAYROLL2 in library PAYROLL renamed as PAYROLL/PAYRAISE
ftp>
```

Administrator: Command Prompt - ftp earl

```
ftp: 2262 bytes sent in 0.22Seconds 10.14Kbytes/sec.
ftp> cd /home
Connection closed by remote host.
ftp> open earl
Connected to earl.example.com.
220-QTCP at earl.example.com.
220 Connection will close if idle more than 5 minutes.
501 OPTS unsuccessful; specified subcommand not recognized.
User (earl.example.com:(none)): sandi
331 Enter password.
Password:
230 SANDI logged on.
ftp> bin
200 Representation type is binary IMAGE.
ftp> del payroll/payroll2
250 File PAYROLL2 in library PAYROLL deleted.
ftp>
```



helpsystems

Build a Transactional Firewall

The function of an **exit program** can be to do anything (even malicious!) as it's written by a programmer; however, for network (PC) access, security officers typically want it to:

1. **Audit** (as IBM i doesn't do a good job on its own)
2. **Control** (as object security is often weak or lacking)

The exit program returns a ***pass/fail*** indicator to the exit point which then halts or continues the transaction's journey.

NOTE: A "pass" does not mean the transaction will be honored. The request still has to satisfy OLS rules assuming they exist.

Do We Really Need Exit Programs?

Exit programs compensate for—and reduce the risk associated with—poorly configured security controls.

Deploy exit programs to:

- Prevent unwanted access to data and commands.
- Allow beneficial and approved access.

They may also:

- Log and alert upon network access attempts.

Okay, So How Do I Get Exit Programs?

Option 1: **Write Your Own**

- IBM provides samples at http://www-01.ibm.com/support/docview.wss?uid=nas8N1018050
- Search the web for published examples
- Can be complex for anything other than simple “block all traffic” type
- Can cause performance issues (esp. with ODBC)
- Should be tested against each OS release
- Auditors often take exception to self-policing

Option 2: **Purchase A Commercial Solution**

Powertech Exit Point Manager for IBM i

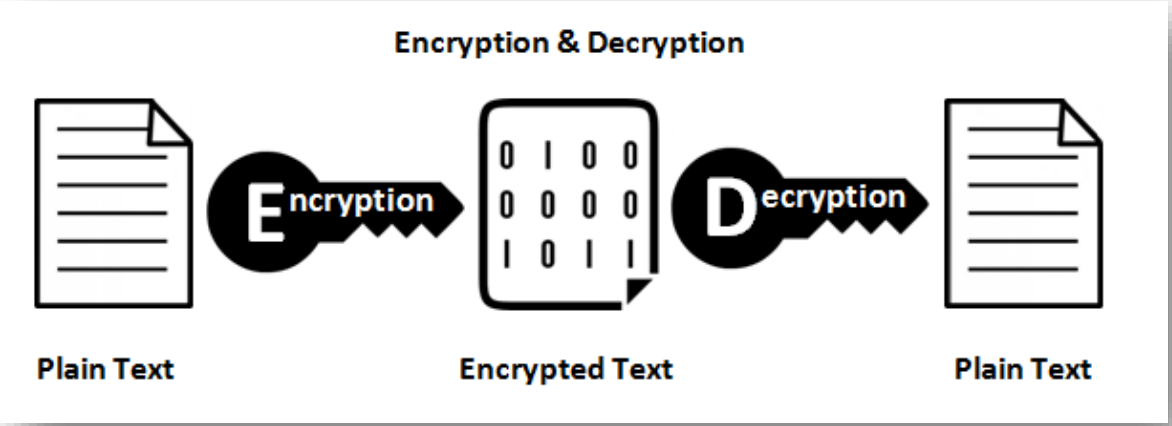
All Data Is Not Created Equal

Data Classification identifies the *sensitivity level* of data

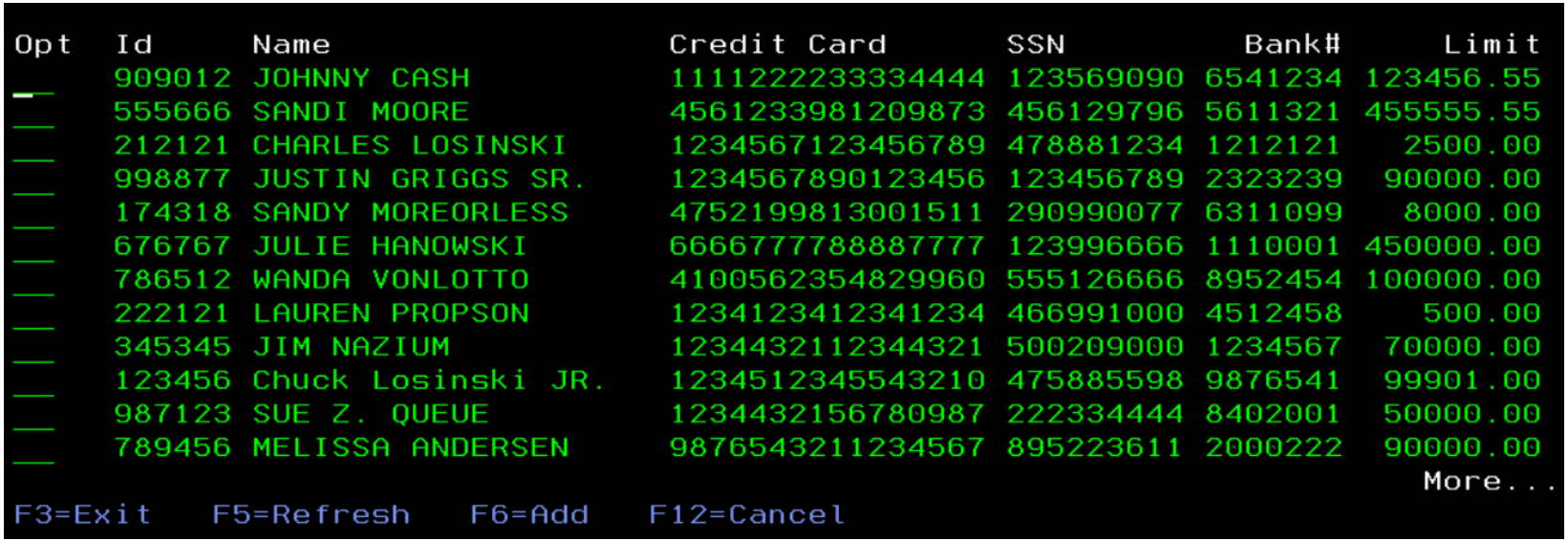
Control access to data and apply security controls based on its classification

Encrypt When Needed

- ✓ Db2 database enhancements and Field Procedures introduced in IBM i v7.1 provide seamless encryption for **CONFIDENTIAL** and **RESTRICTED** data



Application Data – Non-Protected View

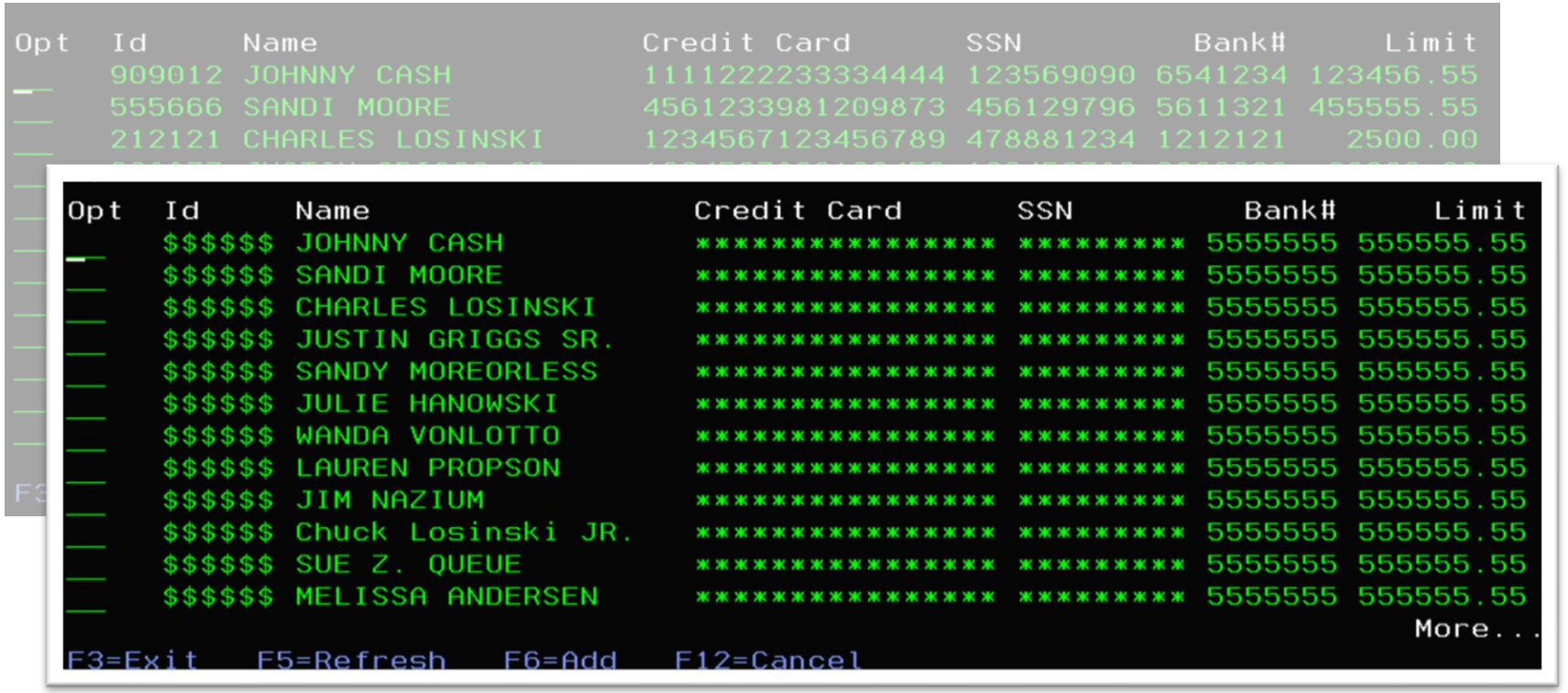


Opt	Id	Name	Credit Card	SSN	Bank#	Limit
_	909012	JOHNNY CASH	1111222233334444	123569090	6541234	123456.55
_	555666	SANDI MOORE	4561233981209873	456129796	5611321	455555.55
_	212121	CHARLES LOSINSKI	1234567123456789	478881234	1212121	2500.00
_	998877	JUSTIN GRIGGS SR.	1234567890123456	123456789	2323239	90000.00
_	174318	SANDY MOREORLESS	4752199813001511	290990077	6311099	8000.00
_	676767	JULIE HANOWSKI	6666777788887777	123996666	1110001	450000.00
_	786512	WANDA VONLOTTO	4100562354829960	555126666	8952454	100000.00
_	222121	LAUREN PROPSON	1234123412341234	466991000	4512458	500.00
_	345345	JIM NAZIUM	1234432112344321	500209000	1234567	70000.00
_	123456	Chuck Losinski JR.	1234512345543210	475885598	9876541	99901.00
_	987123	SUE Z. QUEUE	1234432156780987	222334444	8402001	50000.00
_	789456	MELISSA ANDERSEN	9876543211234567	895223611	2000222	90000.00

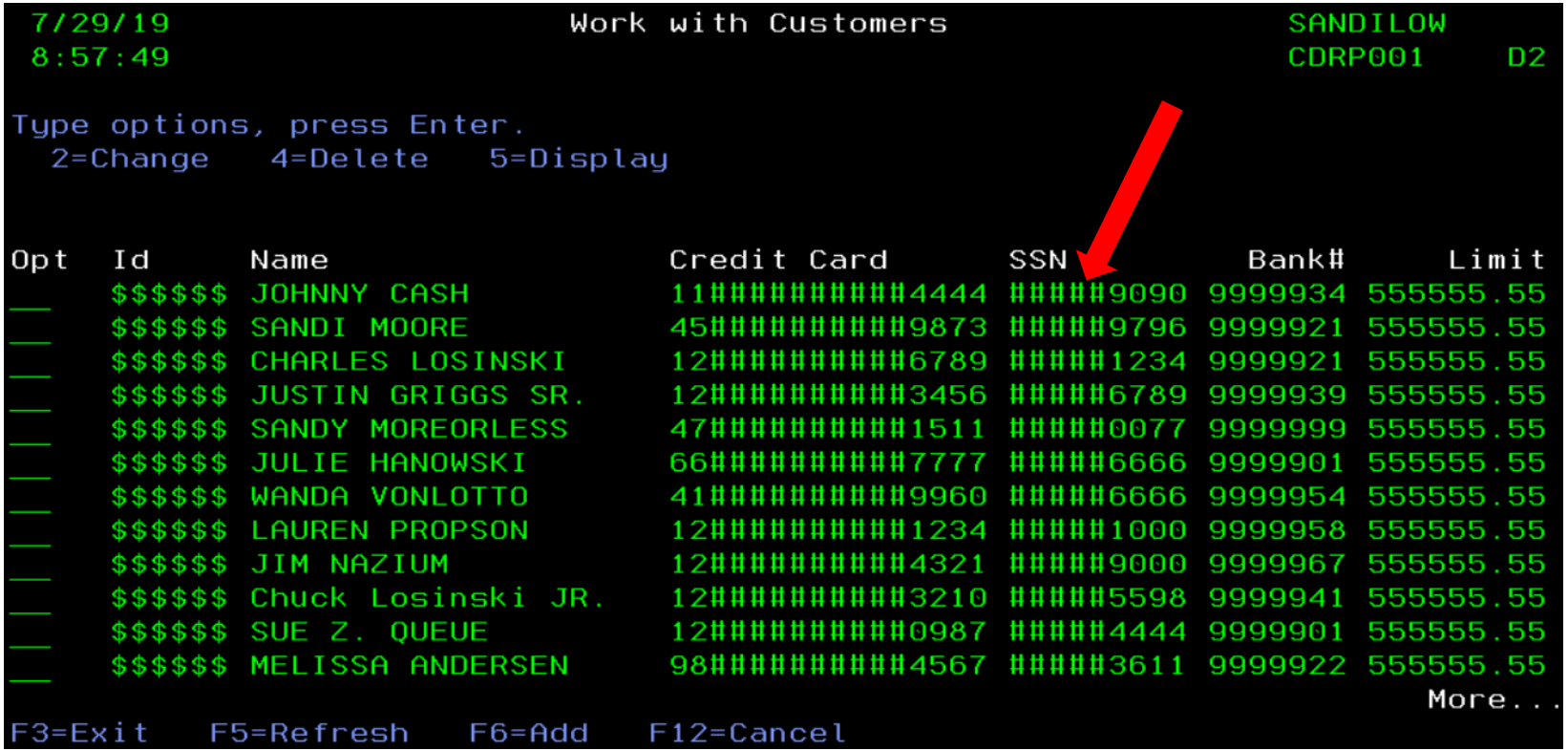
More...

F3=Exit F5=Refresh F6=Add F12=Cancel

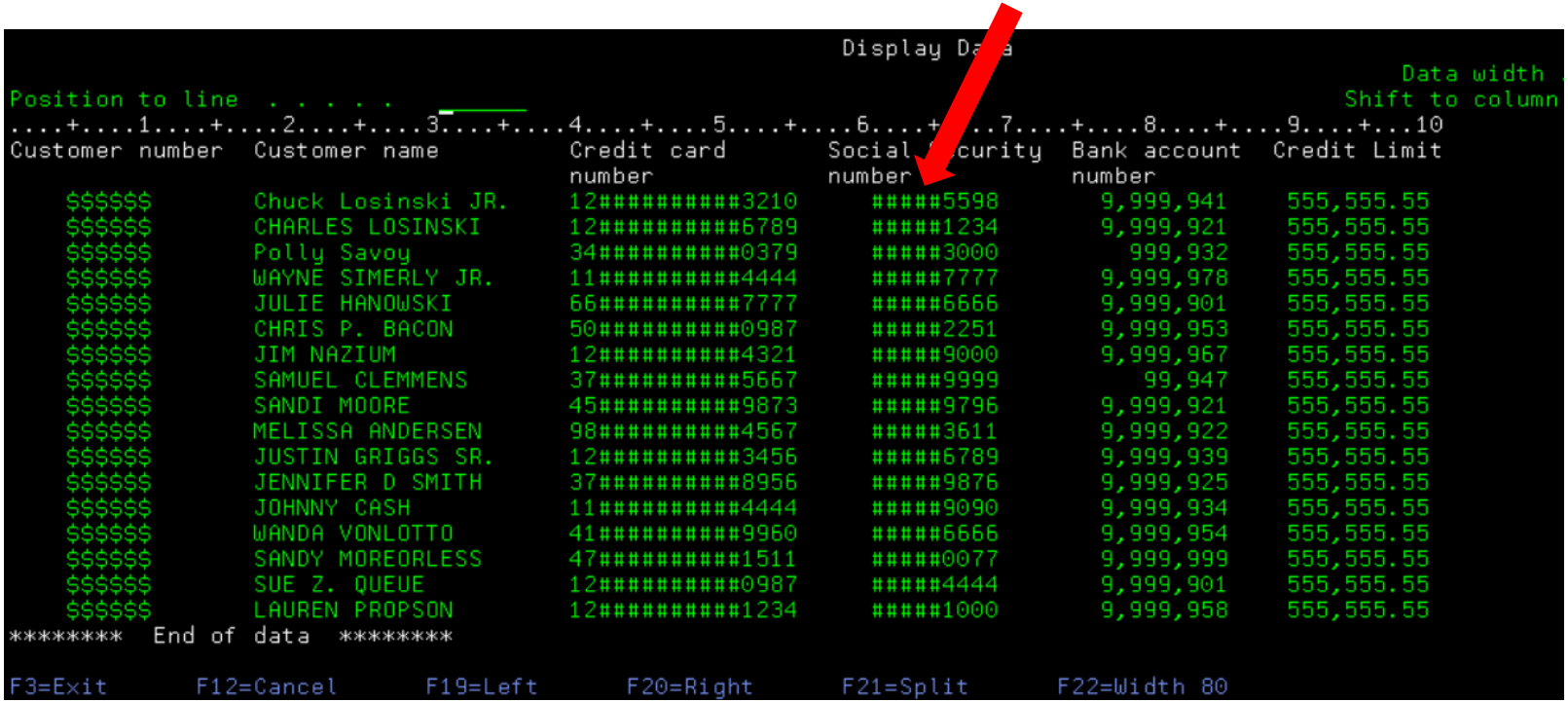
Application Data – Protected (Unauthorized) View



Application Data – Masked View



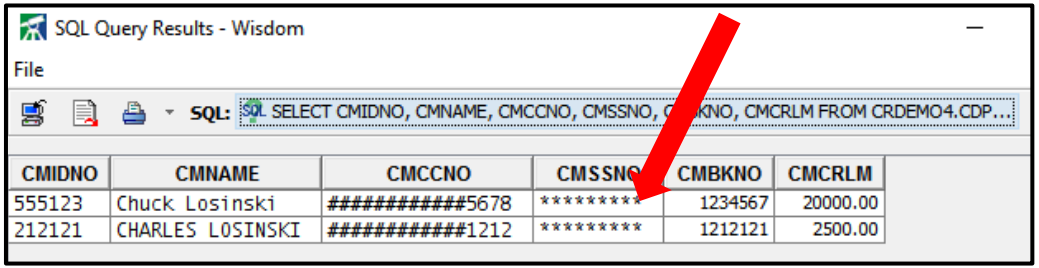
Application Data – Masked View (QUERY/SQL)



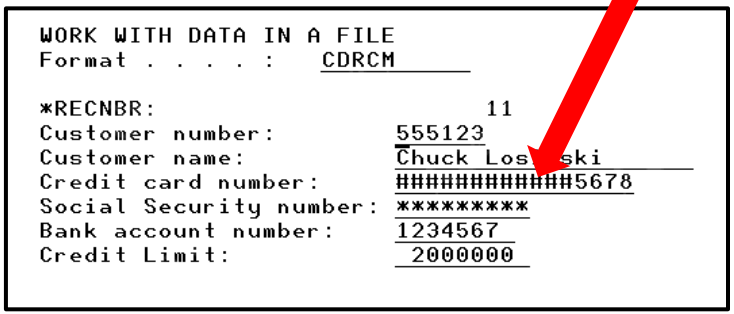
```
                                        Display Data
                                                                        Data width
Position to line  . . . . .                                            Shift to column
....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+...10
Customer number  Customer name          Credit card      Social Security  Bank account  Credit Limit
                                        number           number           number
    $$$$$$       Chuck Losinski JR.     12##########3210    #####5598       9,999,941    555,555.55
    $$$$$$       CHARLES LOSINSKI       12##########6789    #####1234       9,999,921    555,555.55
    $$$$$$       Polly Savoy            34##########0379    #####3000         999,932    555,555.55
    $$$$$$       WAYNE SIMERLY JR.      11##########4444    #####7777       9,999,978    555,555.55
    $$$$$$       JULIE HANOWSKI         66##########7777    #####6666       9,999,901    555,555.55
    $$$$$$       CHRIS P. BACON         50##########0987    #####2251       9,999,953    555,555.55
    $$$$$$       JIM NAZIUM             12##########4321    #####9000       9,999,967    555,555.55
    $$$$$$       SAMUEL CLEMMENS        37##########5667    #####9999          99,947    555,555.55
    $$$$$$       SANDI MOORE            45##########9873    #####9796       9,999,921    555,555.55
    $$$$$$       MELISSA ANDERSEN       98##########4567    #####3611       9,999,922    555,555.55
    $$$$$$       JUSTIN GRIGGS SR.      12##########3456    #####6789       9,999,939    555,555.55
    $$$$$$       JENNIFER D SMITH       37##########8956    #####9876       9,999,925    555,555.55
    $$$$$$       JOHNNY CASH            11##########4444    #####9090       9,999,934    555,555.55
    $$$$$$       WANDA VONLOTTO         41##########9960    #####6666       9,999,954    555,555.55
    $$$$$$       SANDY MOREORLESS       47##########1511    #####0077       9,999,999    555,555.55
    $$$$$$       SUE Z. QUEUE           12##########0987    #####4444       9,999,901    555,555.55
    $$$$$$       LAUREN PROPSON         12##########1234    #####1000       9,999,958    555,555.55
********  End of data  ********

F3=Exit      F12=Cancel      F19=Left      F20=Right      F21=Split      F22=Width 80
```

helpsystems

Application Data – Masked View (Other Tools)



SQL via ODBC or JDBC



Data File Utility (DFU)

helpsystems

Okay, So How Do I Encrypt Data at the Field Level?

Option 1: **DIY**

- Can be very difficult and time-consuming to implement a custom encryption solution
- IBM's APIs are complex and require a lot of research to implement correctly
- Major application changes often needed to encrypt and decrypt data
- Encrypted data contains special characters that interferes with 5250 emulators
- Custom key management solution often does not meet PCI requirements
- Audit trails are non-existent or limited
- Programmers know too much about custom solution – separation of duties

Option 2: **Purchase A Commercial Solution**

Powertech Encryption for IBM i

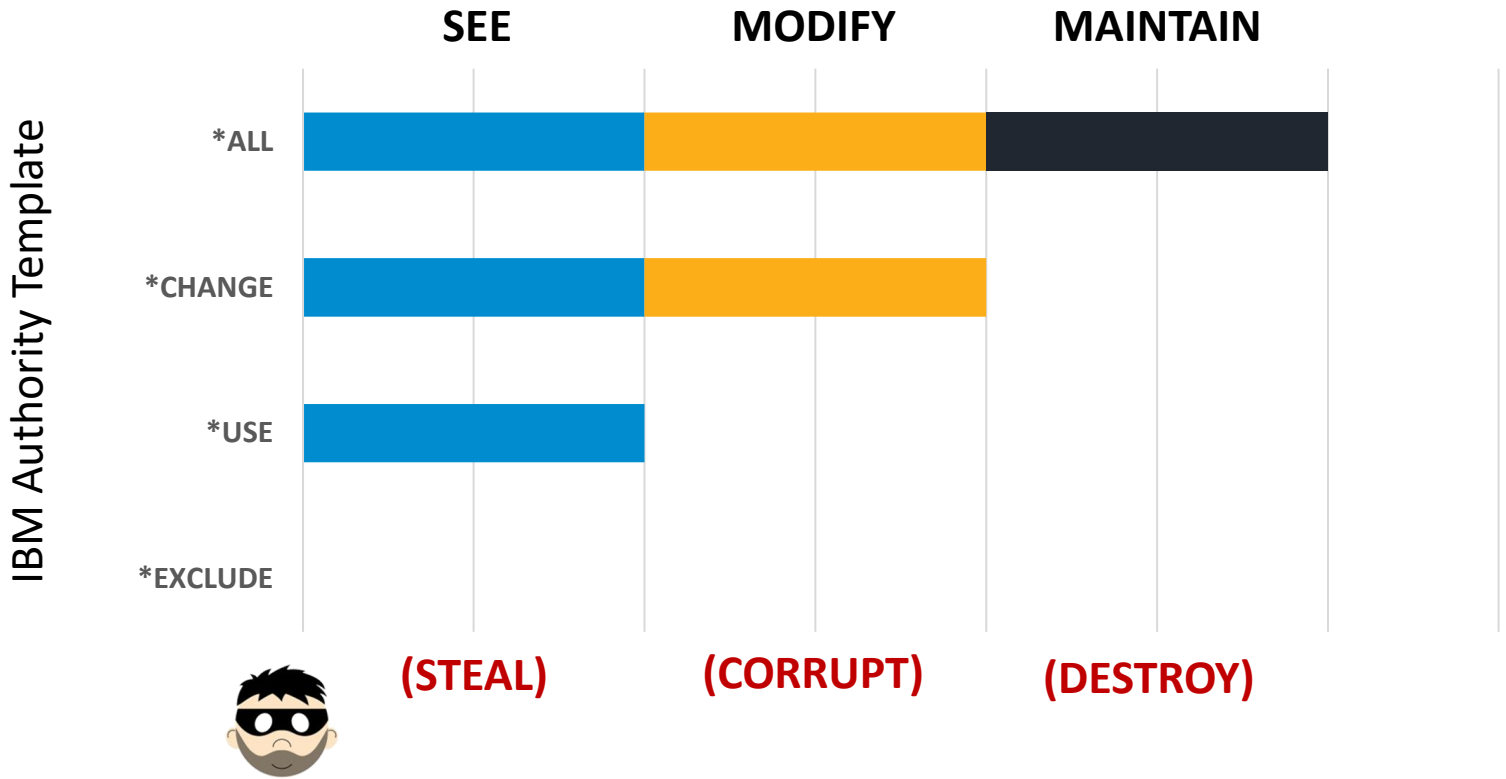
Malware Attacks

A virus cannot **INFECT** or **ENCRYPT** the native library structures under QSYS.LIB but it can **DESTROY** other file systems!

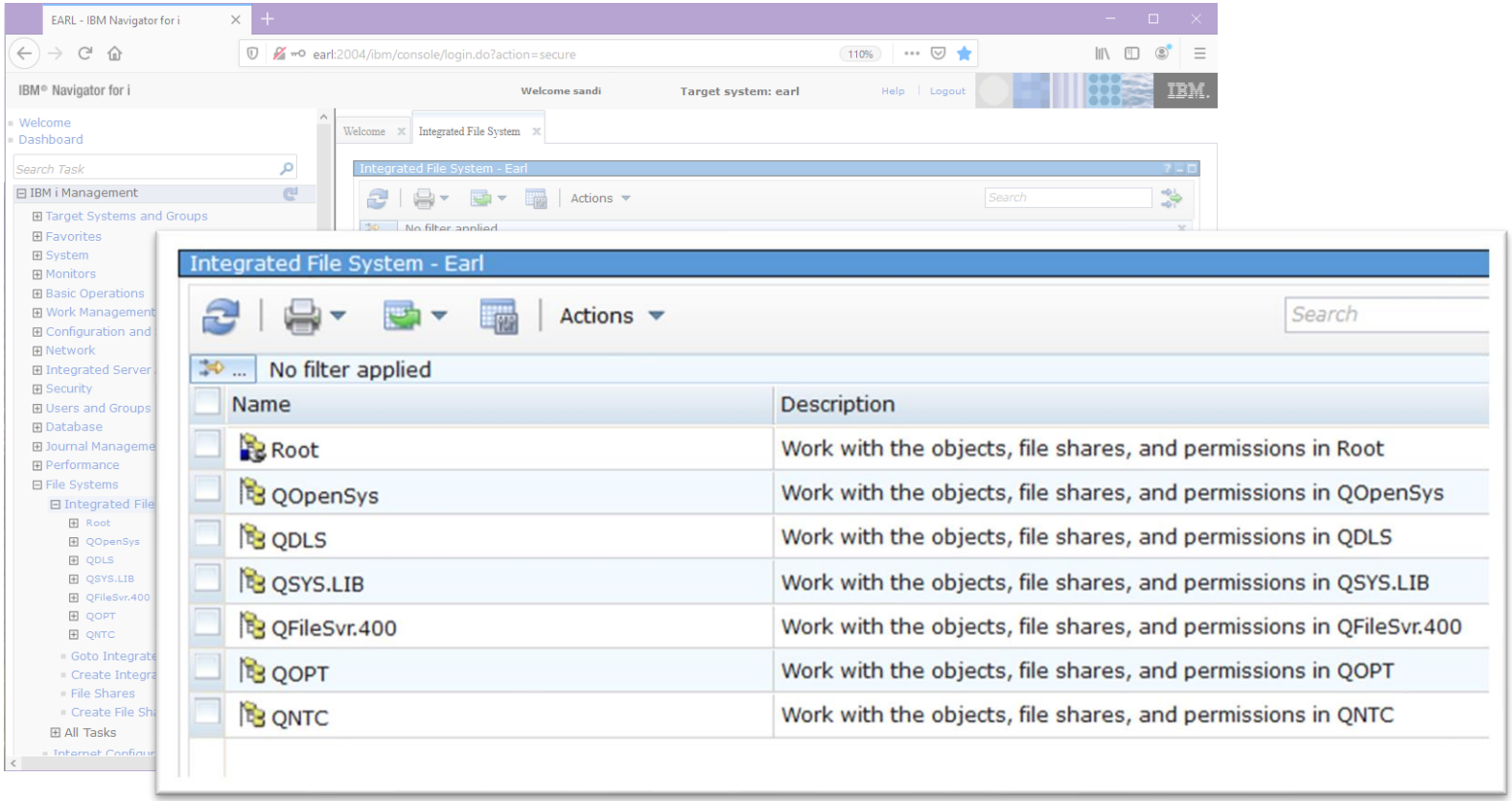
Malicious code can negatively **IMPACT** even the native structures via a rename or a delete operation!

```
Browse : /StandGuard/./LOGS/System virus scan task.log
Record : 747947   of  747960 by  14          Column :   1    132 by  79
Control : _____________________________________________________________

....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....
 Skipped . . : 0
 Errors  . . : 105
 Infected  . : 248095

 Cleaned . . : 0
 Moved . . . : 248095
 Deleted . . : 0

1  File is locked or cannot be opened.
104  Caller denied engine access to either scan or repair.

Completed at Saturday, Aug 01 08:55 PM
2282743 files processed in 78947 seconds (28.91 files/sec)
Task 'System virus scan task' completed with errors. 248095 virus(es) found, 0 f
 ************End of Data**********************

 F3=Exit   F10=Display Hex   F12=Exit  F15=Services  F16=Repeat find
 F19=Left   F20=Right
 1 records folded.
```

IBM i Object-Level Security - Authority Shortcuts



What Objects Malware can Impact

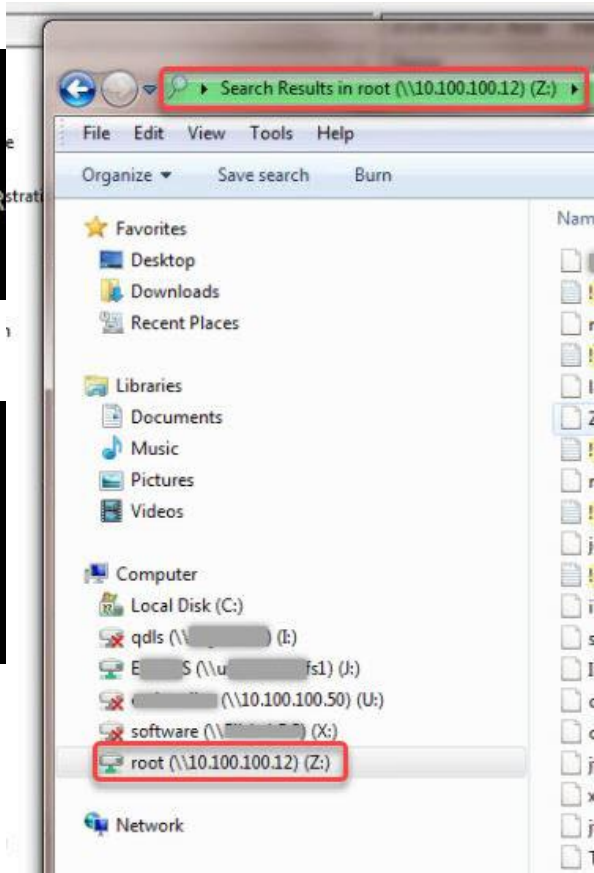


helpsystems

Ways Malware can Impact Objects

```
230 SANDI logged on.
ftp> bin
200 Representation type is binary IMAGE.
ftp> rename payroll/payroll2 payroll/payraise
350 RNFR file PAYROLL2 in library PAYROLL accepted. Type new name using R
250 File PAYROLL2 in library PAYROLL renamed as PAYROLL/PAYRAISE.
ftp>
```

```
Password:
230 SANDI logged on.
ftp> bin
200 Representation type is binary IMAGE.
ftp> del payroll/payroll2
250 File PAYROLL2 in library PAYROLL deleted.
ftp>
```



OK, How Should I Protect the IFS?

- Shut down unused services
- Use exit programs to restrict and audit activities pertaining to IFS-based information
- Avoid sharing '/' (root) and /QSYS.LIB
- Leverage the QPWFSERVER authorization list and consider *PUBLIC(*EXCLUDE)
- Enable system auditing to detect failed connection attempts
- Enable object auditing for sensitive objects in the IFS
- Monitor the audit log so you'll know right away
- Get good backups (and test recovery!)

Don’t Rely On High Availability

Primary

Does your DR Plan accommodate this scary scenario?

Secondary

helpsystems

Next Steps

How can we help?

Things to do next:

- Have your system assessed for common vulnerabilities (HelpSystems does this for FREE)
- Determine if Object Level Security is an appropriate mitigation response.
- Download the current “State of IBM i Security” study.
- Download the CIS Benchmark document for your OS release (available for v7.2 thru v7.4)
- Prioritize all mitigation activities with measurable goals and attainable timelines.
- Evaluate if your team has the necessary expertise and time, else partner up with outside experts.

FREE Annual Exam

SECURITY SCAN

No Obligation

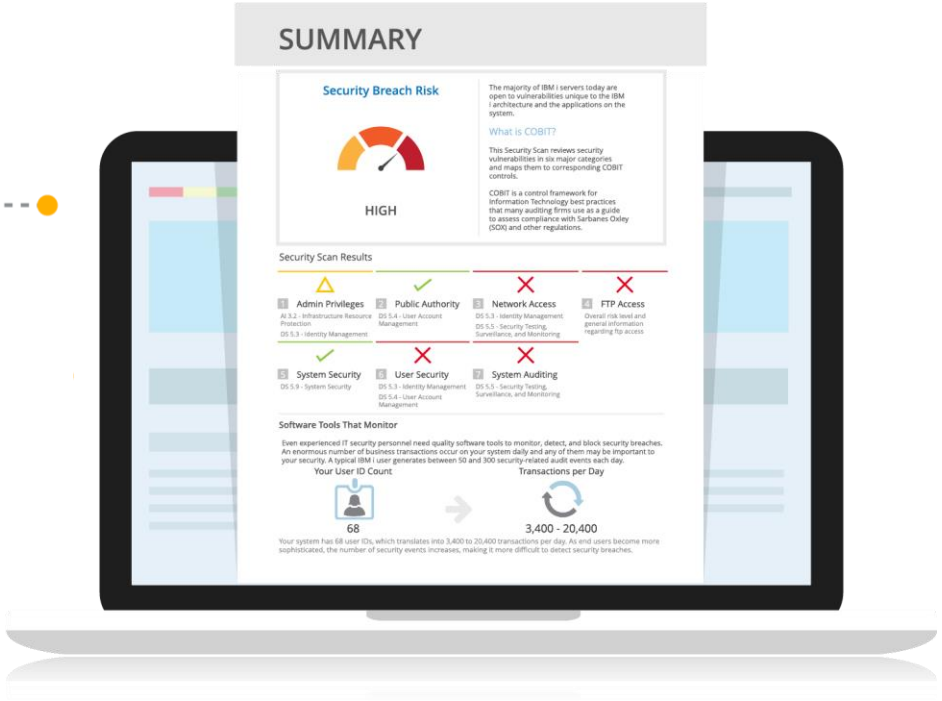
Fast! (~1 minute)

Non-intrusive

Includes expert review

Free 7 Day License

No Cost



helpsystems

helpsystems
Let us help you Build a Better IT™

ANY QUESTIONS?

helpsystems
Let us help you Build a Better IT™

Thank you for joining us

www.helpsystems.com

info@helpsystems.com