i5/OS Security 101

I5/OS Security 101

- **System Level Security**
- **User & Group profiles**
- **Object Level Authorities**

I5/OS Security

- **Security Levels (10, 20, 30, 40, 50)**
- **D.O.D. C2 Security Rating**
- **User Profiles, Group Profiles**
- **Resource Security**
  - » **Specified when objects are created**
  - » **Evaluated when object requested**
- **Security Officer**
- **Security Administrator**
- **Security Auditing Capabilities**

i5/OS Security Levels

WRKSYSVAL QSECURITY

or

DSPSYSVAL QSECURITY

- **10 No system-enforced security (OS/400 V4 Restriction)**
- **20 Sign-on security**
- **30 Sign-on and resource security**

Not Secure

- **40 Sign-on and resource security; Operating system integrity protection**
- **50 Sign-on and resource security; Operating system enhanced protection**

Secure

I5/OS Security Related System Values

- **Major system options and default values**
  Like combined config.sys - system.ini - win.ini in MS/Windows
- **WRKSYSVAL, DSPSYSVAL, CHGSYSVAL, RTVSYSVAL**
- **Various Categories**
  - » Security
  - » **System Control**
  - » **Library List**
  - » **Message**
  - » **etc . . .**

See Appendix A for Security System Values

Resource Security

- **Requires System Security Level 30 and higher**
- **To authorize user access to an AS/400 object**
  - **Command, Program, File, etc.**

Resource Security Options

- **AUT(*ALL)**
- **AUT(*CHANGE)**
- **AUT(*USE)**
- **AUT(*EXCLUDE)**

Object Owner has *ALL authority

IBM Supplied User Profiles

- **QSECOFR** — **God of any AS/400**
- **QSYSOPR** — **The System Operator**
- **QPGMR** — **Programmer**
- **QUSER** — **End-User**
- **QSRV** — **Service**
- **QSRVBAS** — **Service**
- **Many others used for IBM internal Jobs**
  - » **Not Sign-on Enabled**
  - » **QSYS, QTCP, QTMHHTTP**

Other Security Options

- **Adoption of Authority**
  - » **Specified when a program is created, or changed**
- **Security API's**
  - » **Get Profile Handle**
  - » **Change Active Profile**
  - » **Release Profile Handle**
- **Network Security**
  - » **Exit Point Procedures**
  - » **WRKREGINF** Work with Registration Information

User Profiles

- **The User Profile**
  - » **User Profile Attributes**
    - Special authorities
    - User classes
    - Other Attributes
- **Group profiles**
- **Commands for User Profiles**
- **Object ownership**
- **Adopted authority**
- **Assumed identities**
- **Restoring authorities**

The User Profile

- **Determines what the user is allowed to do**
- **Determines how the user's actions are recorded**
  - » **Log level, log CL commands, security audit log entries**
- **Contains information to adapt the system for the user**
  - » **Assistance level, initial menu, initial program, attention program**
- **Contains information about the user's authority**
  - » **Private authorities, special authorities**
- **Identifies the user's jobs and printer output**
  - » **Job and reports are identified as *userid/number/jobname***
- **Can be a member in up to 16 group profiles**

Initial Menus/Programs

- **Initial menus and programs are set in the user profile**
- **Initial menu = *SIGNOFF causes user to signoff when initial program ends**
- **User *may* be able to specify alternate initial menus and programs from the signon screen**

Limited Capability Users

- Limited Capabilities Users *YES
  Cannot change initial program or initial menu
  Can only enter certain commands on an AS/400 command line
  - Sign off (SIGNOFF)
  - Send message (SNDMSG)
  - Display messages (DSPMSG)
  - Display job (DSPJOB)
  - Display job log (DSPJOBLOG)
  - Work with Messages (WRKMSG)
- Partially Limited Capabilities Users *PARTIAL
  Can Change Initial Menu
  Can Enter Commands
- To enable Limited Users to use other CL commands, use the command (CHGCMD)

Special Authorities

- **User profiles can be assigned special authorities**
  - ***ALLOBJ – allows access to all resource on the system**
  - ***SECADM – ability to manage user profiles**
  - ***JOBCTL – control all jobs and IPL the system**
  - ***SPLCTL – control all spool files, and jobs in job queues**
  - ***SAVSYS – ability to save and restore any object**
  - ***SERVICE – ability to run STRSST command**
  - ***AUDIT – control all system auditing functions**
  - ***IOSYSCFG – configure system communications**

- ***ALLOBJ and *SPLCTL Special authority trump object authorities**

User Classes

- **Used to set default special authorities and to determine menu options seen**
  - ***USER – none**
  - ***SYSOPR – *JOBCTL, *SAVSYS**
  - ***PGMR – none**
  - ***SECADM – *SECADM, *JOBCTL, *SAVSYS**
  - ***SECOFR – all special authorities**

User Profile Commands

- **Commands to manipulate user profiles**
  - **CRTUSRPRF – Create user profile**
  - **CHGUSRPRF – Change user profile**
  - **DLTUSRPRF – Delete user profile**
  - **DSPUSRPRF – Display user profile**
  - **RSTUSRPRF – Restore user profile**
  - **RTVUSRPRF – Retrieve user profile**
  - **WRKUSRPRF – Work with user profiles**

CRTUSRPRF Command

- **Create user profile**
- **Used to create new profiles**
- **Must have security administrator (*SECADM) special authority**
- **Cannot give the profile special authorities you don’t have**

CHGUSRPRF Command

- **Change user profile**
- **Used to change an existing profile**
- **Must have *CHANGE authority to the user profile**
- **Must have security administrator (*SECADM) special authority**
- **Cannot give the profile special authorities you don't have**

DLTUSRPRF Command

- **Delete user profile**
- **Used to delete profiles**
- **Must have *OBJEXT and *USE authority to the user profile**
- **Must have security administrator (*SECADM) special authority**
- **You can delete a profile that has special authorities you don't have**
- **Must determine what to do with Owned Objects**

DSPUSRPRF Command

- **Display user profile**
- **Used to display existing profiles**
- **Must have *USE authority to the user profile**

RSTUSRPRF Command

- **Restore user profile**
- **Used to restore user profiles from backup media**
- **Must have *OBJEXT to replace an existing profile**
- **Must have save/restore special authority**
- **The owner of the profile must be known to the system**
- **Must run the RSTAUT command to restore authorities**

RTVUSRPRF Command

- **Retrieve user profile**
- **Used to retrieve profile attributes into a CL program**
- **Similar to the DSPUSRPRF, just used in a program**
- **Must have *USE authority to the user profile**
  - » **Remember, you can become any profile to which you have *USE authority**

WRKUSRPRF Command

- **Work with user profiles**
- **Used to display, change, or delete existing profiles**
  - » **In general 'work with' commands provide great flexibility**
- **Must have *USE authority to the user profile to even see it**
- **Must have appropriate authority to change or delete the profile**
- **You can *become* any profile to which you have *USE authority! See next page.**

Hijacking a User Profile

- **A user with sufficient authority to another user profile, can run jobs as that user.**

- **WRKUSRPRF….. Who do you see?**

RSTAUT Command

- Restore authorities
- Private authorities stored in a user profile
- Use only after a RSTOBJ/RSTLIB and RSTUSRPRF
- Requires a dedicated system
- When you restore a system, don’t forget it!

Group Profiles

- **Group profiles can be used to give several people the same level of authority**
- **Support for primary group profile, and up to 15 supplemental group profiles**
- **Group profiles should not have passwords**
- **Group profiles should not own production objects – They should be owned by an Owning Profile**
- **A member of the group has all the rights that the group has**
  - » **Including special authorities**

Object Ownership

- **Every object has an owner**
- **The owner typically has *ALL authority to an object**
- **The owner of an object will always have authority to modify authorities**
  - » **Even when the owner has *EXCLUDE rights to the object**
- **Restored objects have their ownership stripped if their owner is not recognized. QDFTOWN is owner**

Adopted Authority

- **Adopted authority allows the user who executes a program to adopt the authority of the program's owner**
- **Useful in tightly scripted programs that provide access to a single function**
- **Done through the USRPRF(*OWNER) parameter on CRTxxxPGM or the CHGPGM commands.**

Adopted Authority

- **Adopted authority is cumulative**
- **IFS does not support adopted authority**
- **The program owner's authority and special authorities are adopted.**

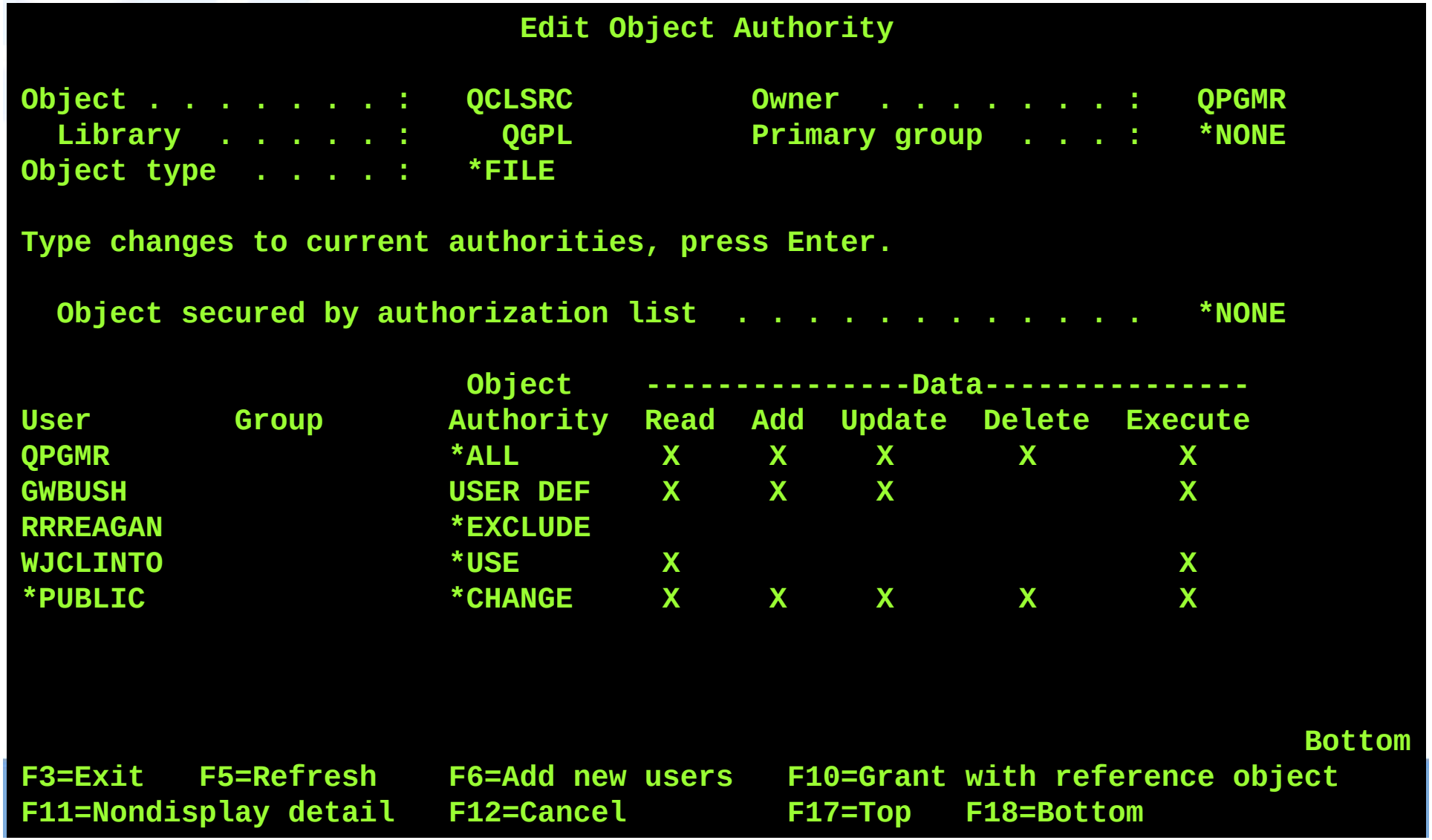
Object Level Authorities

- **Data authorities**
- **Object authorities**
- **CL security commands for native objects**
- **CL security commands for IFS objects**
- **Authority shortcuts**
- **Authorization lists**

Data Authorities

- **Read**
  - » **Access the contents of the object**
- **Add**
  - » **Add entries to the object**
- **Update**
  - » **Change the content of object**
- **Delete**
  - » **Remove entries from the object**
- **Execute**
  - » **Run a program or search library**

Data Authorities EDTOBJAUT



Object Authorities

- **Operational (Opr)**
  - » **Right to *use* the object**
- **Management (Mgt)**
  - » **Right to control the object**
- **Existence (Exist)**
  - » **Right to delete the object**
- **Alter**
  - » **Right to alter the object (triggers)**
- **Reference (Ref)**
  - » **Right to use as referential constraint**

Object Authorities

Object Oriented Architecture

- **Control Language (CL) security commands for native objects**
  - **DSPOBJAUT – Display object authority**
  - **EDTOBJAUT – Edit object authority**
  - **GRTOBJAUT – Grant object authority**
  - **RVKOBJAUT – Revoke object authority**
  - **WRKOBJ – Work with object**

Object Oriented Architecture

- **CL security commands for IFS objects**
  - **CHGAUT – Change authority (IFS)**
  - **WRKAUT – Work with authority (IFS)**
  - **WRKLNK – Work with link (IFS)**

Authorization Shortcuts

- ***USE – Read rights**
- ***CHANGE – Change rights**
- ***ALL – Total rights to object and data**
- ***EXCLUDE – No rights to object or data**
- **USER DEF – User defined combination**
- ***AUTL – Rights for *PUBLIC listed in an authorization list**

*USE Authorization

- ***USE authorization provides**
  - **Read – access the contents of the object**
  - **Execute – run a program or search a library**
  - **Operational – right to *use* the object)**

- **Can be trumped by special authorities**

*CHANGE Authorization

- ***CHANGE authorization provides**
  - **Read – access the contents of the object**
  - **Add – add entries to the object**
  - **Update – change the contents of the object**
  - **Delete – remove entries from the object**
  - **Execute – run a program or search a library**
  - **Operational – right to use the object**
  - **Reference – right to use as referential constraint**
- **Can be trumped by special authorities**

*ALL Authorization

- ***ALL authorization provides**
  - » **Read – access the contents of the object**
  - » **Add – add entries to the object**
  - » **Update – change the contents of the object**
  - » **Delete – remove entries from the object**
  - » **Execute – run a program or search a library**
  - » **Operational – right to use the object**
  - » **Management – right to control the object**
  - » **Existence – right to delete the object**
  - » **Alter – right to alter the object (triggers)**
  - » **Reference – right to use as referential constraint**

*EXCLUDE Authorization

- ***EXCLUDE authorization provides**
  - » ***No* authority to the object**
    - Cannot even see the object, but…
    - Can verify object's existence with the CHKOBJ command
- **Can be trumped by special authorities**

USER DEF Authorization

- **USER DEF authorization provides**
  - » **Any other combination of data and object authorities that you choose**

- **Can be trumped by special authorities**

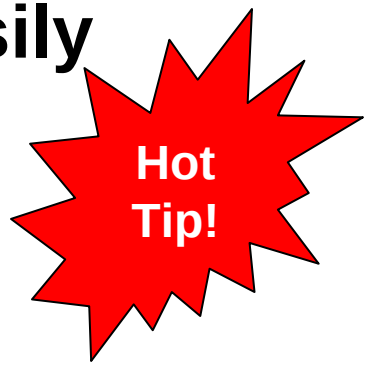
*AUTL Authorization

- ***AUTL authorization**
  - **The public's authority to the object is set by an authorization list**
    - An authorization list can only be specified for *PUBLIC
- **Can be trumped by special authorities**

Authorization Lists

- Used to grant object authority to like objects
- Typical authorization list uses
  - » Secure all the programs in a library
  - » Secure files in a library to one particular group for *USE, and another group for *CHANGE

- Use authorization lists and group profiles together to create a flexible, yet easily managed security system



Authorization Lists

EDTAUTL
Command

```
                          Edit Authorization List

Object . . . . . :   EXAMPLE          Owner  . . . . . :   QSECOFR
  Library  . . . . :     QSYS          Primary group  . . :   *NONE

Type changes to current authorities, press Enter.

             Object    List  ----------Object-----------
User        Authority  Mgt   Opr  Mgt  Exist  Alter  Ref
QSECOFR     *ALL        X     X    X     X      X     X
GWBUSH      USER DEF    X     X    X
RRREAGAN    *EXCLUDE
WJCLINTO    *USE              X
*PUBLIC     *CHANGE           X

                                                                  Bottom
F3=Exit      F5=Refresh   F6=Add new users   F11=Display data authorities
F12=Cancel   F15=Display authorization list objects   F17=Top   F18=Bottom
```

Can Manage the list

Authorization Lists

```
                          Edit Authorization List

Object . . . . . :   EXAMPLE          Owner  . . . . . :   QSECOFR
  Library  . . . . :     QSYS          Primary group  . . :   *NONE

Type changes to current authorities, press Enter.

             Object    ---------------Data---------------
User         Authority  Read  Add  Update  Delete  Execute
QSECOFR      *ALL        X     X     X       X        X
GWBUSH       USER DEF    X     X     X                X
RRREAGAN     *EXCLUDE
WJCLINTO     *USE        X                            X
*PUBLIC      *CHANGE     X     X     X       X        X

                                                                  Bottom
F3=Exit   F5=Refresh   F6=Add new users   F11=Nondisplay detail   F12=Cancel
F15=Display authorization list objects    F17=Top   F18=Bottom
```

Authorization Lists

```
                    Display Authorization List Objects

Authorization list . . . . . :   SGIPGM
  Library  . . . . . :     QSYS
Owner  . . . . . :   SGIOBJOWN
Primary group  . . . . . :   *NONE

                                                  Primary
Object      Library     Type      Owner           group       Text
HSMCLT1     STRATEGI    *PGM      SGIOBJOWN       *NONE       HSM Test Client (1,0
HSMCLT2     STRATEGI    *PGM      SGIOBJOWN       *NONE       HSM Test Client (10,
HSMCLT3     STRATEGI    *PGM      SGIOBJOWN       *NONE       HSM Test Client (*PI
HSMCLT4     STRATEGI    *PGM      SGIOBJOWN       *NONE       HSM Test Client (SHO
HSMCLT5     STRATEGI    *PGM      SGIOBJOWN       *NONE       HSM Test Client (1,0
HSMRCVRP    STRATEGI    *PGM      SGIOBJOWN       *NONE       HSM Client Send Requ
HSMRCVRQ    STRATEGI    *PGM      SGIOBJOWN       *NONE       HSM Server Receive R
HSMSKLC     STRATEGI    *PGM      SGIOBJOWN       *NONE       Skeleton HSM Server
HSMSKLCL    STRATEGI    *PGM      SGIOBJOWN       *NONE       Skeleton HSM Server
HSMSKLRPG   STRATEGI    *PGM      SGIOBJOWN       *NONE       Skeleton HSM Server
                                                                        More...
Press Enter to continue.

F3=Exit    F12=Cancel    F17=Top    F18=Bottom
```

Questions?