SKYVIEW PARTNERS, LLC

World Class Security Experts

Step by Step Approach to Implementing Object Level Security

Carol Woodbury, President and Co-Founder

SkyView Partners

carol.woodbury@skyviewpartners.com

www.skyviewpartners.com

Agenda

- **How to you start**
- **Popular application security schemes**
- **Secure security schemes**
- **How to avoid breakage**

SKYVIEW PARTNERS, LLC

www.skyviewpartners.com

Who and what … ?

- **Who (what type of user) is using the application?**
  - Order entry clerk
  - System operator
  - System administrator
- **What are they using it for?**
  - Take orders including credit card numbers
  - Manage the system
  - Administer employee data base including social security numbers
- **What interfaces need to access the data?**
  - EDI
  - Web applications
  - Other host-based applications
  - ODBC
  - FTP

SKY VIEW PARTNERS, LLC

Determine your data access policy

- **What type of data is being stored?**
  - Private data
  - Company proprietary
  - General information

Who should be allowed to see this data outside of the application?

- No one unless they are coming through the application that manages the data
- Only employees with a direct job requirement
- Anyone in the company

- **Should anyone be allowed to modify the data outside of the application?**
  - Probably not

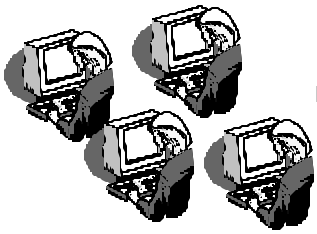
SKY VIEW PARTNERS, LLC

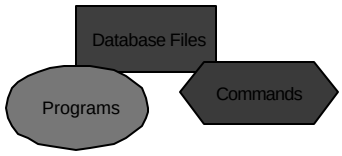
Popular implementations for menu “security”

- *ALLOBJ
- Group ownership
- *PUBLIC authority

SKYVIEW PARTNERS, LLC

Reliance on *ALLOBJ





***ALLOBJ**

***ALL access to all application objects**

Plus ... everything else on the system

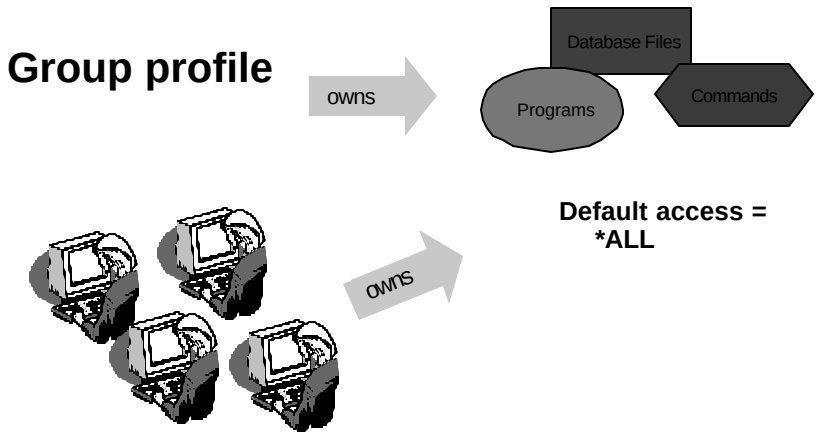
SKYVIEW PARTNERS, LLC

Steps to change from *ALLOBJ

- Set appropriate *PUBLIC authority
- Create a user profile that does not have *ALLOBJ
- Test
- Remove *ALLOBJ special authority for application users

SKYVIEW PARTNERS, LLC

Reliance on Group Ownership

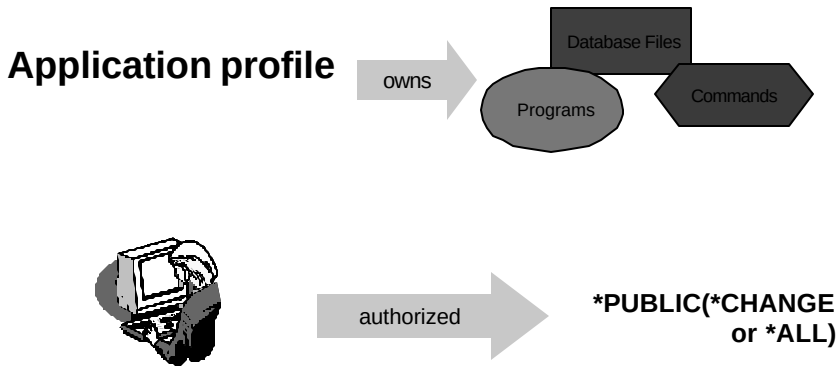


SKYVIEW PARTNERS, LLC

Steps to change from group ownership

- **Define and implement new authorization model**
- **Set appropriate *PUBLIC authority**
- **Create a user profile that is not a member of the application owning profile**
- **Test**
- **Remove users from application owning profile group**

Reliance on *PUBLIC authority



Steps to change from wide-open *PUBLIC authority

- **If you must test in production environment *TEMPORARILY* make users members of application owning profile**
- **Set new *PUBLIC authority**
- **Create a user profile that is not a member of the application owning profile**
- **Test**
- **Remove users from application owning profile group**

SKY VIEW PARTNERS, LLC

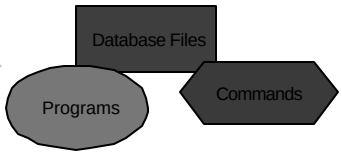
Authorization methods for secure applications

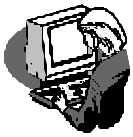
- **Adopted authority – "Application only access"**
- **qsysetgid() API**
- **Swap profile**

SKY VIEW PARTNERS, LLC

Application only access

Application profile owns





authorized to

***PUBLIC(*EXCLUDE)**

- **Initial program**
- **Programs adopt**
- **Owner owns or is authorized to all application objects**

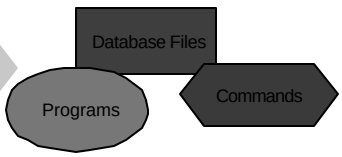
Disadvantage:

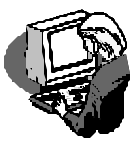
- **Absolutely no access to objects via network interfaces**

SKY VIEW PARTNERS, LLC

Variations on application only access

Application profile owns





authorized to

***PUBLIC(*EXCLUDE)**

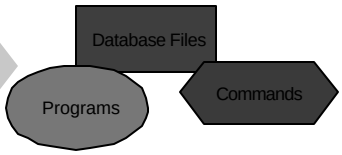
- **Some files**
- **Query libraries**

To allow access via ODBC, FTP

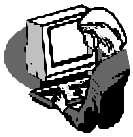
SKY VIEW PARTNERS, LLC

Variations on application only access

Application profile owns



***PUBLIC(*USE)**



authorized for

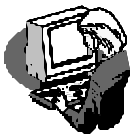
Update - *CHANGE

- **Some files**
- **Query libraries**

To allow access via ODBC, FTP

SKYVIEW PARTNERS, LLC

Swap profile



becomes

Application profile

- Application profile owns or is authorized to all application objects

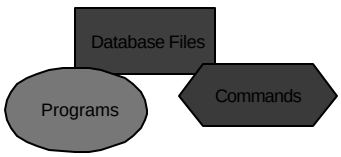
User initiating request

Advantage:

- **Works with IFS**

Disadvantages:

- **Audit entries logged under application profile**
- **Job user name stays as original**



***PUBLIC(*EXCLUDE)**

SKYVIEW PARTNERS, LLC

Swap profile – profile handle APIs

SALLY
- **SAL_GRP_1**
- **SAL_GRP_2**
- **SAL_GRP_3**

swaps to

JOE
- **JOE_GRP_1**
- **JOE_GRP_2**
- **JOE_GRP_3**

Using QSYGETPH and QWTSETP APIs

- User
- All groups
- Limited capability
- Special authorities

Restrictions:

- **Handle cannot be passed between jobs**

SKYVIEW PARTNERS, LLC

Swap profile – profile token APIs

SALLY
- **SAL_GRP_1**
- **SAL_GRP_2**
- **SAL_GRP_3**

swaps to

JOE
- **JOE_GRP_1**
- **JOE_GRP_2**
- **JOE_GRP_3**

Using QSYGENPT and QSYSETPT APIs

- User
- All groups
- Limited capability
- Special authorities

Advantages:

- **Can be passed between jobs**
- **Configured to time-out or be one - time use**

Disadvantages:

- **Slightly less secure**
- **Slightly more difficult to use**

SKYVIEW PARTNERS, LLC

Swap profile – uid and gid APIs

SALLY
- **SAL_GRP_1**
- **SAL_GRP_2**
- **SAL_GRP_3**

swaps to

JOE
- **SAL_GRP_1**
- **SAL_GRP_2**
- **SAL_GRP_3**

using qsysetuid()

SALLY
- **SAL_GRP_1**
- **SAL_GRP_2**
- **SAL_GRP_3**

swaps to

SALLY
- **APP_PROF**
- **SAL_GRP_2**
- **SAL_GRP_3**

using qsysetgid()

SKYVIEW PARTNERS, LLC

Application profile

- **Create a profile whose sole purpose is to own the application**
  - No password -- PWD(*NONE)
  - No special authorities -- SPCAUT(*NONE)
  - No group profile – GRPPRF(*NONE)
- **Do not use IBM profiles to own your application objects!!!**

QSECOFR	QTCP
QSYS	QPGMR
QSRVBAS	QSRV
QSYSOPR	QUSER

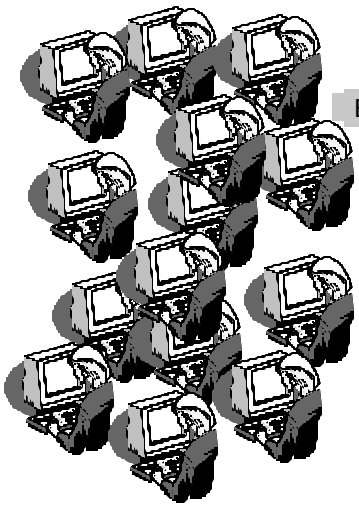
SKYVIEW PARTNERS, LLC

If not the whole application, then part

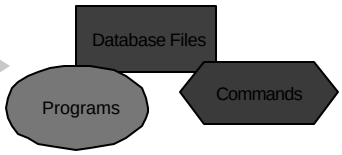
- **Start securing at the library or directory level**
  - *PUBLIC(*EXCLUDE)
  - Give application users
    - *USE to library
    - *RX to directory (*X to directories in the path)
  - Don't touch the objects in the library or directory

SKY VIEW PARTNERS, LLC

Here's the current configuration …



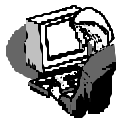
Everyone

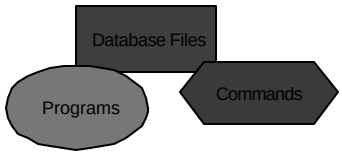


Payroll Library
***PUBLIC(*ALL)**

SKY VIEW PARTNERS, LLC

Here's where to end up …





PAY_GROUP

Considerations:

- Other applications may need access to the library
- Other users may need access to the data

Payroll Library

***PUBLIC(*EXCLUDE)**

PAY_GROUP *USE

Preventing breakage

- **Analyze what interfaces need to access the data**
  - ODBC
  - FTP
  - DDM
- **Are there individuals who need additional authorities?**
- **Map out all job scheduled entries for**
  - General idea of the job
  - User under which the job runs
  - Job description
  - Library list

Before changing a vendor application

- **Contact the vendor**
  - May already have an architected solution
  - May choose to no longer support your installation of you make authorization changes
- **Requirements if changing to use adopted authority:**
  - Prior to V5R1-compiled code:
    - Source *or*
    - Observability
  - Can always re-translate V5R1 and later code

SKY VIEW PARTNERS, LLC

Detecting breakage

- **Use DSPAUDJRNE or**
- **CRTDUPOBJ of QSYS/QASYxxJ5 then**
  - DSPJRN JRN(QSYS/QAUDJRN) RCVRNG(*CURCHAIN) FROMTIME('08/18/2004' '08:00:00') JRNCDE((T)) ENTTYP(AF) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE5) OUTFILE(SKYVIEW/QASYAFJ5)
- **Hint: Look at these entries BEFORE you start making changes!**

SKY VIEW PARTNERS, LLC

Accommodations

- **Programmer access to**
  - update production data - in “emergencies”
  - read production data – for debug
  - read production source
- **EDI**
- **FTP processes**
- **On-call users needing to view joblog of *ALLOBJ users**
- **On-call users needing to DSPUSRPRF**

SKYVIEW PARTNERS, LLC

Security Project

- **You WILL be the target and accused of whatever is going wrong at the moment**

SKYVIEW PARTNERS, LLC

For More Information

- **Basic Security – iSeries Infocenter**
  - www.iseries.ibm.com/infocenter
- **iSeries Security Reference, SC41-5302**
- **Experts' Guide to OS/400 Security by Carol Woodbury and Patrick Botz, 29th Street Press, 2004, ISBN 1-58304-096-X**

SKY VIEW PARTNERS, LLC