SKYVIEW PARTNERS, LLC

World Class Security Experts

Top Security Issues Facing OS/400 and i5/OS Security Administrators Today

Carol Woodbury, President and Co-Founder

SkyView Partners

carol.woodbury@skyviewpartners.com

www.skyviewpartners.com

No security policy

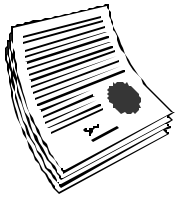
- **Causes:**
  - Confusion
  - Lack of direction
  - Conflict

SKYVIEW PARTNERS, LLC

www.skyviewpartners.com

Security policy – Key issues

- **Assigns responsibility**
- **Requires:**
  - Buy-in from top management
  - Regular review and updates
    - Especially when adding new technology, e.g., Internet access, wireless communications, video-enabled cell phones, etc
  - Communication to all employees
  - Enforcement



SKY VIEW PARTNERS, LLC

Technology isn't always the answer

- **Technology may not yet exist to solve problem**
  - DoS or Virus detection
- **Technology may be too complex**
  - Single sign on (password synchronization solutions)
  - Digital certificates
- **Technology cannot enforce all aspects of security policy**
  - Cannot prevent sharing of data to which a user is authorized
  - Cannot control users' behavior

SKY VIEW PARTNERS, LLC

Profiles are out of control !!!

- Old profiles
- Profiles with default passwords
- Inappropriate special authorities
- Inappropriate group assignments
- Publically authorized profiles

SKY VIEW PARTNERS, LLC

Old profiles

- Profiles remain on the system even though the person has left the company or the profile is no longer needed
- Look at both Last sign on date and Last used date to analyze
- Use ANZPRFACT to keep system clean

SKY VIEW PARTNERS, LLC

Default passwords

- **Use ANZDFTPWD to detect**
  - These are the first passwords a hacker will try
- **Set one of the password system values to prevent users from changing to a default value**
- **Change the PASSWORD parameter of CRTUSRPRF to be *NONE**

Inappropriate use of special authorities

- **Special authorities give users the ability to perform some function – for example, configure auditing, manage spooled files, etc.**
- ***ALLOBJ special authority gives the user the ability to access ANY object on the system.**

***ALLOBJ = DANGER !!!**

- **Don't give users special authorities by default.**
- **Stop copying profiles without looking at the special authorities**
- **Don't give *SPLCTL just to share printed output**

Special authority definitions

- **ALLOBJ**
  - Can access ***EVERY*** object on the system.
- ***AUDIT**
  - Configure audit values.
- ***IOSYSCFG**
  - Manage and configure everything to do with TCP/IP and networking.
- ***JOBCTL**
  - Control all aspects of all jobs on the system.
- ***SAVRST**
  - Save or restore any object whether or not they have authority to do so.
- ***SECADM**
  - Create and manage user profiles.
- ***SERVICE**
  - Use system service tools.
- ***SPLCTL**
  - The *ALLOBJ of spooled files

SKYVIEW PARTNERS, LLC

Pretending to be Someone Else

Can be accomplished by:

- **Sharing user ids and passwords**
- **User profile named in a jobd at security level 30**
- ***USE to a profile allows you to**
  - Submit a job
  - Swap to another profile
    - Profile swap APIs
    - Profile token APIs
    - setuid / setgid APIs

SKYVIEW PARTNERS, LLC

Taking control of your users

- **Determine if *USE authority is appropriate for profiles**
  - Use PRTPUBAUT to get a list
- **Analyze who actually needs each special authority (Don't be fooled - they'll say they need them all!)**
  - Use PRTUSRPRF to get list of profiles and their special authorities
- **Don't forget to analyze group profiles**
  - Use DSPAUTUSR to get a list of group profiles and members

SKYVIEW PARTNERS, LLC

Taking control of your users

OS/400 commands:

- ANZDFTPWD – Analyze default password
  - *DISABLE
  - Expire password
- ANZPRFACT – Analyze profile activity
  - List only
  - *DISABLE
- CHGEXPSCDE – Change expiration schedule entry
  - Disable
  - Delete
- CHGACTSCD – Change activation schedule entry
  - Disable / Enable at specific times

Operations Navigator

- Simplified creation/deletion/management of user profiles

Management Central

- Password synchronization
- Automatic profile update after change
- "Post" commands can run after profile creation
- Copy user profile between systems

SKYVIEW PARTNERS, LLC

DST passwords

Change DST passwords

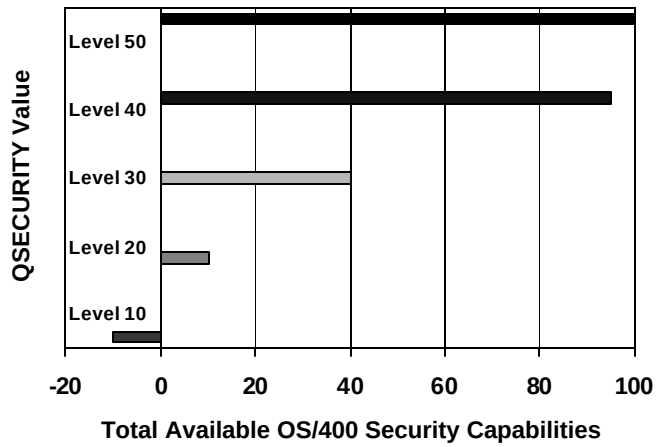
- **DST – Dedicated Service Tools are very powerful – You need to change these passwords as well.**

QSECOFR	**QSECOFR**
QSRV	**QSRV**
11111111	**11111111**
22222222	**22222222**

- **V5R1 allows you to customize DST access, define Service tools ids to allow access to DST and SST**
- **Note: As of V5R1 DST password were case sensitive !!!**

SKY VIEW PARTNERS, LLC

Running at the wrong security level (QSECURITY)



SKY VIEW PARTNERS, LLC

Changing your security level

- **Moving from security level 30 to security level 40 or 50**
  - Turn on *PGMFAIL auditing
    - Look for AF B, C, D, R, S audit entries
  - Manage JOBDs that name user profiles
    - Use PRTJOBDAUT (Print Job Description Authority)
    - Look for AF J audit entries
  - Change QSECURITY
  - IPL
- **Moving from security level 20 takes careful planning to determine where authority is going to come from**

Unsecured copies of production data

- **Developers need copies to test against**
  - Data is often “real”
  - Copies are often left unsecured on test machines or on media
- **May be exposing private data**

Programmer access to production systems

- **Programmers have access using powerful profile for debugging purposes**
- **No auditing or exception reporting in place.**
- **Source code is often on production machines for "emergencies"**
  - If left on production, must be secured!

SKY VIEW PARTNERS, LLC

Programmer access to production systems

- **Policy issue**
- **Needs to be the exception, not the rule**
- **Processes needed to log**
- **Audit the programmers' activity**

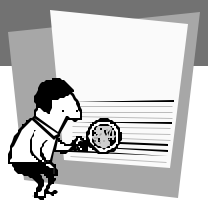
SKY VIEW PARTNERS, LLC

No trace, no trail …

- **If you don't audit, you have no records of what happened**
- **May need to audit to meet regulations**
- **Caution – don't audit too much!**

SKY VIEW PARTNERS, LLC

Auditing…



Can configure auditing by:

- System-wide actions
- User actions
- Use of an object
- Use of an object by user

- **OS/400 system values**
  - QAUDLVL
    - Sets action auditing
  - QAUDCTL
    - On / Off switch for auditing
- **OS/400 commands**
  - CHGSECAUD – Change Security Auditing
    - Set up auditing
  - DSPSECAUD – Display Security Auditing
    - Display audit journal entries (QAUDJRN)
  - CHGUSRAUD – Change User Auditing
  - CHGOBJAUD – Change Object Auditing
- **Minimum recommendation:**
  - *SECURITY (use *SECCFG and *SECRUN in i5/OS), *SAVRST, *AUTFAIL, *DELETE, *CREATE, *SERVICE – trying to audit the exceptions, not the rules

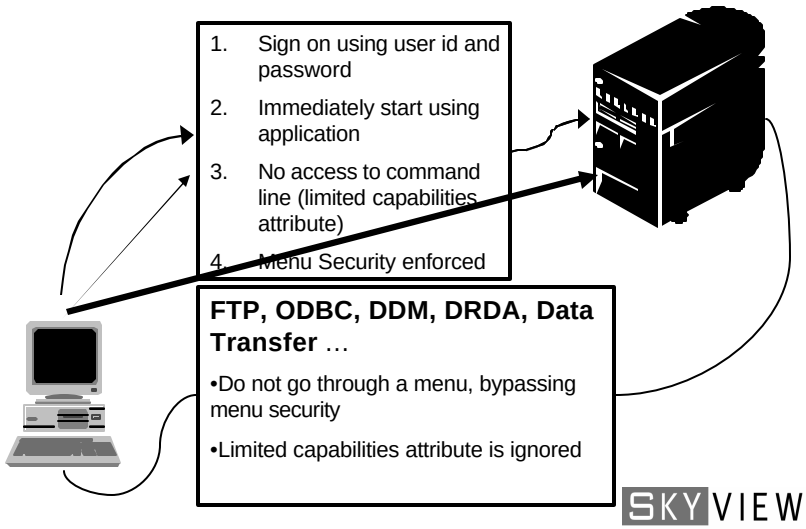
SKY VIEW PARTNERS, LLC

Reliance on Menu "Security"

- **Menu 'Security' is based on:**
  - The original architecture of AS/400 – that is, no network access by end-users
  - Limited capability attribute is strictly enforced
  - Robust security scheme within the application itself enforces security policy

SKY VIEW PARTNERS, LLC

Menu Security/Limited Capabilities - Bypassed



SKY VIEW PARTNERS, LLC

Managing what appears on the users' desktop

- **"Green screen" - Menu access control**
  - LMTCPB(*YES)
  - Initial program is application entry
  - Initial menu – *SIGNOFF
- **PC desktop**
  - Application Administration
  - Microsoft Policies
- **Not inherently "bad" but you can't stop there!**

SKY VIEW PARTNERS, LLC

No object level security

Therefore … access to objects defaults to *PUBLIC access

- **Every OS/400 object has a default access called *PUBLIC authority**
- **OS/400 defaults this value to *CHANGE**
- **Most vendors let their objects default to this value or worse, change the default to *ALL**
- **What these values allow:**
  - *USE allows a file to be downloaded
  - *CHANGE allows a to be downloaded, modified and uploaded.
  - *ALL allows the object to be modified, replaced, or deleted

SKY VIEW PARTNERS, LLC

Implementing object level security

Start at the top

- **Determine**
  - What ***type*** of user needs to access each application
  - ***Who*** needs to access the application comes later
- **First examine**
  - Libraries
  - Directories
- **If required, then analyze**
  - Objects within
- **Secure using**
  - *PUBLIC authority
  - Groups
  - Authorization lists
  - Private
- **Tools**
  - QCRTAUT system value
  - Library Create Authority

SKY VIEW PARTNERS, LLC

25

www.skyviewpartners.com

Objects owned by group profiles

- **IF**
  - The GROUP PROFILE owns the objects in a library...
- **AND**
  - A user is a of the member of that group profile…
- **THEN**
  - Every member of the group ‘owns’ every object.

SKY VIEW PARTNERS, LLC

26

www.skyviewpartners.com

Changing an application's security model

- **First check with the vendor to see if a procedure is already in place**
- **Determine the application's authorization model, e.g., group profile, *PUBLIC authority, adopted authority…**
- **Map out your approach**
- **Start slowly**
- **Document your changes**
  - May need to re-apply them with each application upgrade or fix

Caution: may cause adverse reaction from vendor !!!

SKYVIEW PARTNERS, LLC

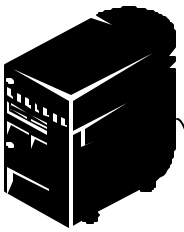
27
www.skyviewpartners.com

Exit programs

Use exit programs when you need

- Additional auditing of transactions
- An additional layer of security on top of object level security

NOT as a substitute for object level security !!!



FTP, ODBC, DDM, DRDA, Data Transfer …

- Do not go through a menu, bypassing menu security
- Limited capabilities attribute is ignored

SKYVIEW PARTNERS, LLC

28
www.skyviewpartners.com

Ignoring the File Systems

- **More OS/400 function is shipped in one of the file systems (such as root ('/')) each release.**
- **Root ('/') is shipped with the equivalent of *PUBLIC(*ALL)**
  - DTAAUT(*RWX)
  - OBJAUT(*ALL)

SKY VIEW PARTNERS, LLC

What to do with the IFS…?

- **Set '/' to no more than**
  - DTAAUT(*RX)
  - OBJAUT(*NONE)
- **Monitor using**
  - PRTPUBAUT
  - PRTPVTAUT
  - DSPAUT
- **Change using**
  - CHGAUT
  - WRKAUT

Don't forget virus scanning !!!

(Virus Got you Down white paper available from www.skyviewpartners.com)

SKY VIEW PARTNERS, LLC

Rampant use of file shares

- File shares make the directory “available” to the network
- Many systems have shared ‘/’
- Manage file shares through iSeries Navigator
- Secure the QZLSADFS (Add file share) and QZLSCHFS (change file share) APIs

TCP/IP applications

If you don’t use a server, don’t start it !

- Check autostart attribute of servers.
  - These will start when STRTCP is run.
- Check authority to STRTCPAPP
  - Once TCP is started, starts all TCP servers regardless of autostart value.

Trojan horses

Can come in the form of

- Exit programs (for network servers)
  - WRKREGINF
  - CHGNETA
- Trigger programs
  - PRTTRGPGM
- Command validation programs
  - WRKKREGINF
  - Command objects
    - Parameter validation programs
    - Prompt override programs

SKYVIEW PARTNERS, LLC

Multiple commands

- **Certain commands are restricted from use …**
  - But have you looked for all instances of it?
  - Or for the UNIX version?
  - Or for the S/38 version?

QSYSV5R1M0
CRTLIB - *CHANGE

QSYSV4R5M0
CRTLIB - *CHANGE

QSYS
CRTLIB - *EXCLUDE

QS38LIB
CRTLIB - *CHANGE

SKYVIEW PARTNERS, LLC

Too many regulations !!!

Sarbanes-Oxley Act

Visa PCI

CA SB 1386

HIPAA

PIPEDA

Basel II

GLBA

The Companies Bill

EU Data Protection Directive

FISMA

SKY VIEW PARTNERS, LLC

35

www.skyviewpartners.com

Regulations Produce Questions

- **Do these regulations apply to me?**
- **What is private data?**
- **Do we retain private data?**
- **What are auditors expecting?**
- **"Recommendations" are so vague, how do I know what to do?**

SKY VIEW PARTNERS, LLC

36

www.skyviewpartners.com

What to Do

- **Need a good security architecture**
- **Start with an assessment**
- **Classify data and identify data owners**
- **Identify areas of weakness**
- **Remediate the weaknesses**
- **Write business justification (risk acceptance statements) for issues not remediated**
- **Documentation, documentation, documentation**
  - Make sure you have a Corporate security policy
  - Document your processes

SKY VIEW PARTNERS, LLC

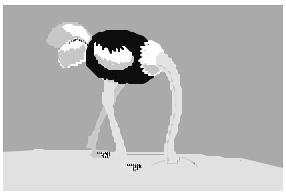
Standards

- **COBIT**
- **ISO17799**

SKY VIEW PARTNERS, LLC

Problems are being Ignored

- **Many people are choosing to ignore the security issues residing on their systems.**
  - "Nothing has happened to my system yet…"
  - Don't want to disrupt production



SKY VIEW PARTNERS, LLC

If you remember one thing …

- **Stop propagating the problem !!!**

SKY VIEW PARTNERS, LLC

For More Information …

- **Security – Basic, SC41-5301**
- **Security – Reference, SC41-5302**
- **Tips and Tools for Securing your AS/400, SC41-5300**
- **Experts' Guide to OS/400 Security by Carol Woodbury and Patrick Botz, ISBN 1-58304-096-X, 29th Street Press 2004.**
- **www.infosecuritymag.com**
- **www.sans.org**
- **www.gocsi.org**
- **www.skyviewpartners.com**

SKY VIEW PARTNERS, LLC