

INTRODUCTION TO THE AS/400

Auditing the AS/400 with Rapport Auditmaster

**Vincent LeVeque
September 1996**

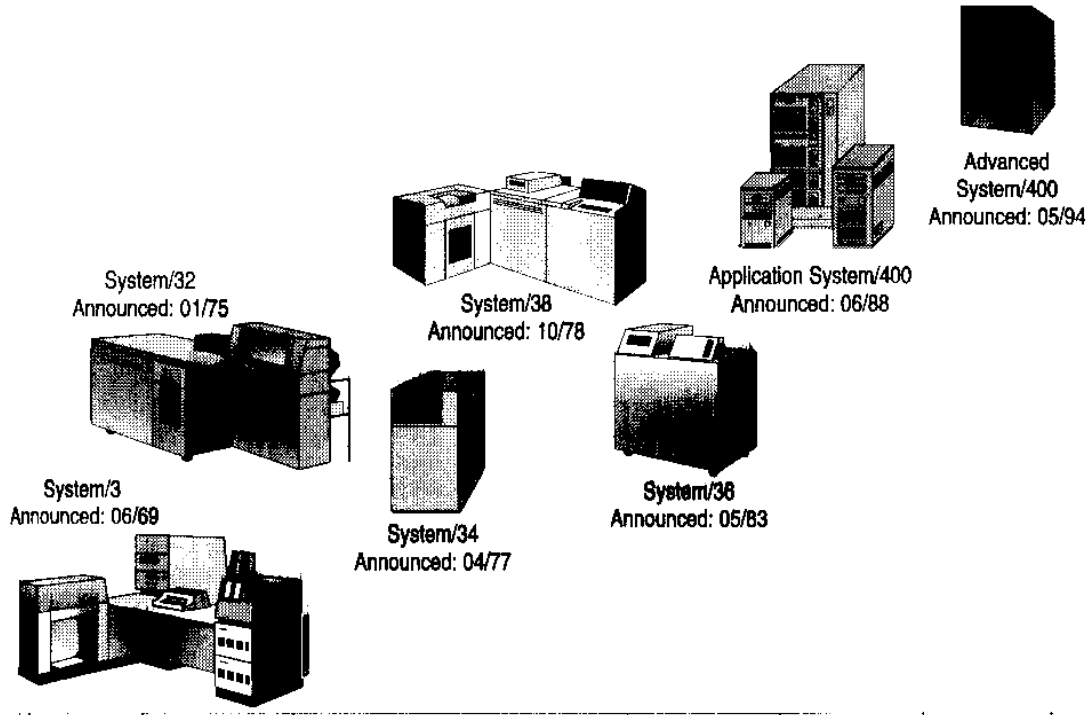
History

- Pre-History: Punch card machines (Unit Record Machines) built by IBM in Rochester, Minnesota
- System/3
 - Offered in 1969
 - Replaced punchcards with disk files and plugboards with RPG
 - Followed by the S/32 then the S/34
- Future Systems Project and the S/38 (object based, integrated database, but poor communications)
 - Originally proposed in 1970
 - Built in Rochester by group entirely separate from S/3
 - Announced in 1978
 - Shipped in 1980
- The S/36 (very popular, abundance of verticle applications, good communications)
 - Over 200,000 sold, many still in use
 - The last “direct descendent” of the S/3

History

- Silverlake "the VAX killer"
 - DEC VAX a threat to IBM in 1980s
 - Market pressure for IBM to integrate and scale product line
 - Silverlake announced as the AS/400 in June 1988
- The “Black Box”
 - Pre-cursor to the RISC-based systems
 - Announced May 1994

History



Product Family

- RISC vs. CISC systems
- Historic CISC processor designations
 - Model series B, C, D, E, F
 - Within a model series, the physical box is designated:
 - 9402, approximately the size of a PC “tower”
 - 9404, approximately the size & shape of a 2-drawer file cabinet.
 - 9406, rack mounted systems
 - Specific model is assigned an alpha plus two digit number (e.g., B10, F60, etc.)
 - Alpha character is model line, higher letters are more recent and powerful models
 - Two digit number is place within an announced line, higher number = more powerful processor

Product Family

- The current line-up

- CISC black box

- 9402 model 200
 - 9406 models 300, 310, 320

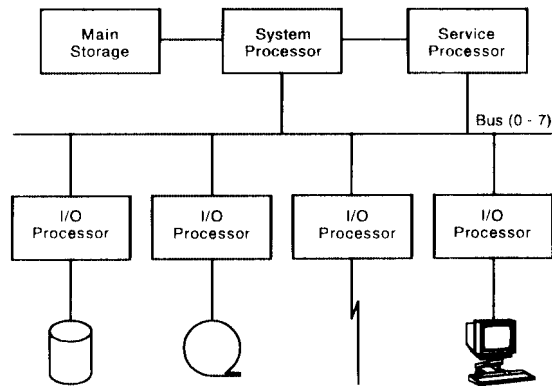
- RISC (PowerPC) box

- 9402 model 400
 - 9404 models 400 and 500
 - 9406 models 500, 510, 530

- Server models - performance optimized for server and batch applications

System Architecture

- Machine Interface (MI) layer isolates hardware from applications
- Multiple processor, 48/64 bit



Operating System Architecture

- Object based
- Consistent, user friendly command/menu interface
- Above & below the Machine Interface
- Single address space (Single Level Storage)
- Integrated relational database

Operating System Versions

CISC AS/400 Systems		RISC AS/400 Systems
"Beige Boxes"	"Black Box"	Future
V3R2	V3R2	V3R7
V3R1	V3R1	V3R6
V2R3	V3R0.5	N/A
Obsolete	N/A	

File System

- Originally only the “AS/400 File System”
- Now multiple file systems are supported

Common Application Software

- Package applications predominate
 - J.D. Edwards
 - Software 2000
 - BPCS
 - MAPICS
 - Lawson
 - Pansophic/PRMS/CA-?
 - JBA
- Custom development
 - RPG/400 or RPG/4 predominant languages
 - More “client server”

Systems Utilities and Tools

■ Programming/Application Development

- CASE tools - Synon, AS/SET, LANSa
- Cross-referencing - Hawkeye
- Off line development - CODE/400

■ Change Management

- Aldon
- Silvon
- Softlanding

■ System Management

- Robot/400
- IBM's Systemview

Business Environment

- Small businesses with turnkey solutions (legacy of S/36)
- Middle market enterprises, approx \$50M to \$500M in gross revenue
- Departmental system in some larger enterprises - run low transaction volume corporate accounting, HR/Payroll, etc.
- Some large corporations are using as data center system
- Early 1990's saw use as mainframe downsizing platform - most activity was 4381 VSE systems migrating.

Recent Trends and Future Prospects

- Move to open standards (TCP/IP, Unix Specs). Internet functionality, relational database features, improved C compiler.
- Some Open Systems vendors now porting to AS/400
- Low end competition from Windows NT and Intel-based UNIX
- Gartner Group report - value proposition, need to keep third party vendors developing. Similar to Macintosh.

The AS/400 Command Use

- The 5250 Keyboard

- Derived from 3270, and ultimately from keypunch machines
- Block mode screens - entirely different from command based ASCII terminals (VT100), not as sophisticated as a GUI.

The AS/400 Command Use

■ Functions of keys:

- Enter Key - submits screen to computer for processing. Computer does not "see" anything you type until you press enter (or a similar key)
- Function Keys - Typically control the operation of the program. Depending on how they are programmed, they may or may not send screen information to computer.

■ Some important function keys:

- PF1 Help. Note help is cursor sensitive, with many AS/400 commands you can get help on the specific field.
- PF3 Cancel, usually gets you entirely out of a menu sequence, but sometimes only out of current screen (see F12)
- PF5 In some commands this will do a screen refresh, especially if the command collects real-time data
- PF9 When you are at a command line, this is recall your previous commands (usually)
- PF11 At a command prompt, will show the parameter keywords.
- PF12 Usually gets you out of your prior screen. Sometimes takes you completely out of the function (see PF3)

How to Log On

The screenshot shows a terminal window with the following content:

Untitled-1: Slot:9Addr:4

Sign On

System : S1010716
Subsystem : QCTL
Display : WN

User _____
Password _____
Program/procedure _____
Menu _____
Current library _____

(C) COPYRIGHT IBM CORP. 1980, 1994.

The bottom status bar contains a cursor icon, the number '6 53', a left arrow icon, and a right arrow icon.

Command Menus

- OS/400 user interface is menu driven
- Default menu set in user profile
- User class (in user profile) determines which menus are permitted
- Useful functions are grouped into menus
- Menus accessed by typing “GO XXXX”, where XXXX is the name of the menu
 - GO PRINTER - gives the spool file and printer management menu
 - GO PROGRAM - gives the programming menu
 - GO SECURITY - gives a menu of basic security management functions

Command Literals

- Hundreds of commands
- All commands have similar derivation
 - Commands composed of 3 character “syllables”
 - First 3 characters describe the action (DSP = display, WRK = work with, etc.)
 - Next 3 characters give object of action, with additional optional 3 character qualifier
 - Sometimes and additional one-letter descriptor (an “adjective”) is appended to the command (e.g., JOB D = Job Description, etc.)
- If you are not sure of a command, it is fairly easy to guess what it is
 - You want a command to change a communications device, try wrkdev, chgdev, etc.
 - That doesn't work, so you try WRKDEV D, work with device description
 - SUCCESS!

Useful Hints for Command Use

- A “work with” command is usually the most general form
- Typing in the command name then pressing “Help” or “F1” will provide help text on the command
- Typing in the command name then pressing “F4” will prompt you for each command parameter
- For some commands, an abbreviated set of parameters is initially presented. To get the full set, press “F10”
- Pressing “Help” or “F1” at any prompt will provide help text on that specific prompt
- Where a prompt has a list of possible values, pressing “F4” will present this list.

Useful Commands

■ System configuration commands:

- DSPHDWPRD - Display hardware products
- DSPSFWRSC - Display software resources
- WRKSYSVAL - Work with system values
- DSPLIB - Display library
 - Can provide a listing of all libraries defined on the system
 - Can also list all objects within a given library

■ System Performance and Usage commands

- WRKSYSSTS - Work with system status
- WRKACTJOB - Work with active jobs
- WRKDSKSTS - Work with disk status

■ Commands to manage your own session

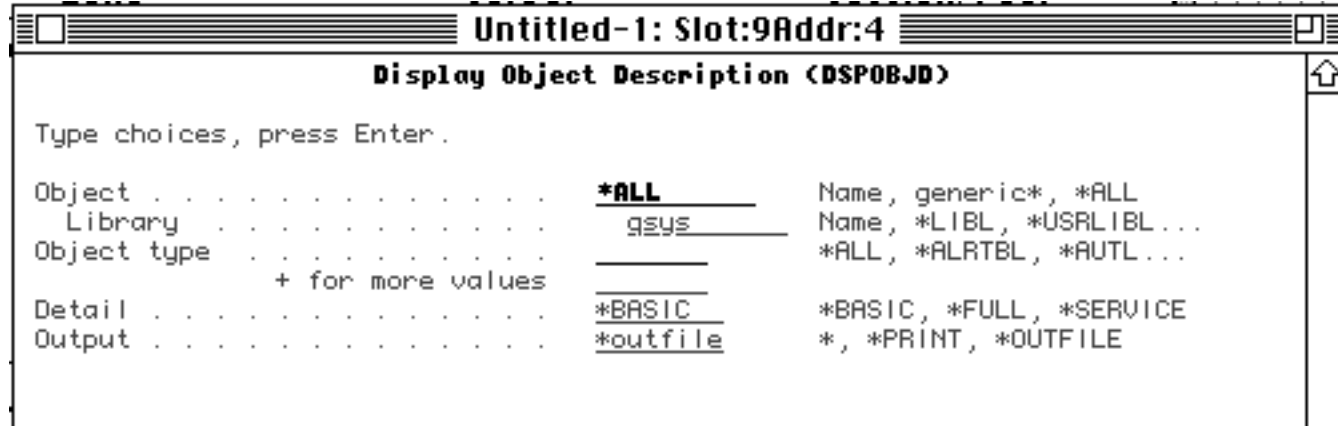
- WRKJOB - Work with jobs; provides ability to view your spool files, job log, etc.
- WRKSBMJOB - Work with submitted jobs; can view spool files, job log of any batch jobs you have submitted

■ Commands to manage the printer and printed output

- WRKOUTQ - Work with output queue

Outfiles and Queries

- Many commands permit sending output to a database file. This file may be later queried for useful reports.
- An outfile is created from the command prompt as follows:
 - First, enter the command, press F4, and enter all parameters. Be sure to specify out as *OUTFILE



Outfiles and Queries

- The, enter the name and library of the outfile.

```
Display Object Description (DSPOBJD)

Type choices, press Enter.

Object . . . . . > CALL          Name, generic*, *ALL
Library . . . . . > QSYS         Name, *LIBL, *USRLIBL...
Object type . . . . . > *cmd       *ALL, *ALRTBL, *AUTL...
                        + for more values
Detail . . . . . *BASIC       *BASIC, *FULL, *SERVICE
Output . . . . . > *OUTFILE    *, *PRINT, *OUTFILE
File to receive output . . . . . output   Name
Library . . . . . kpmgtmp     Name, *LIBL, *CURLIB
Output member options:
Member to receive output . . . *FIRST   Name, *FIRST
Replace or add records . . . . *add    *REPLACE, *ADD
```

I. Exercise - Some Useful AS/400 Commands

Log on to the AS/400 using your assigned user ID and password.

Execute the following commands. Note the results:

1. DSPJOB - Display Job
 - a. Option 4 - Spool files. Do you have any spool files? If so, what are they?
 - b. Option 10 - Job Log. Display your job log. Scroll to the beginning of your session.

2. WRKACTJOB - Work Active Jobs
 - a. Who is on the system right now? Are they interactive or batch users?
 - b. Press F5 to accumulate CPU usage statistics. Is anyone a “CPU Hog”?

3. GO PRINTER - Printed Output Function menu
 - a. What do you think the relationship is between printed output, print queues, and printers?
 - b. What is the device name of the default system printer (hint: try option 6)
 - c. How many output queues are on this system? Which have files waiting to print?
 - d. How many printer devices are on the system? What is their status?

4. WRKDSKSTS - Work with disk status.
 - a. How much total disk space is on the system? What is the percent utilization?

5. WRKHDWPRD - Work with hardware products (Note: This will take some time to run)
 - a. How would this information be useful when conducting a general controls review?

6. DSPSFWRSC - Display Software Resources (note this will take a REALLY long time to run. Go stretch out or have a cup of coffee if you like).
 - a. How would this information be useful when conducting a general controls review?

When you are done, press F3 until you are back at the main menu.

AS/400 SECURITY

- Overall Principles
- System Values
- User Profiles
- Object Authority
- Authorization Lists
- The Security Model
- Application Security
- Communications Basics
- Communications Security

Overall Principles

- All system entities are OBJECTS - Files, programs, commands, device descriptions, job queues, etc.
- Objects have owners, who have privileged rights to the object
- Other owners may be granted specific authority to the object by the owner or a system security officer.
- Any principal not specifically given or denied authority to a specific object gains the default authority assigned to *PUBLIC. *PUBLIC is the “and everyone else authority”
- Certain principals may be given broad authority over entire classes of objects. This is done through “Special Authorities”

System Values

- System Values determine overall operating system characteristics.
 - Security
 - Character set
 - System date and time
 - Default device naming
 - Minimum operating system memory allocation
- System Security Values include:
 - Overall level of security
 - Permitted password characteristics
 - Default library list
 - Auditing of security events
 - Protection of operating system objects and memory (per DoD C2)

User Profiles

- User Profiles provide system access to principals.
- User profiles are required to sign on, to submit a batch job, or to start a communications process.
- User profiles define the initial user environment
 - Initial Program and Menu
 - Print queue, job description, message queue, etc.
- User profiles contain the Special Authorities, which provide broad classes of high level access:
 - *ALLOBJ
 - *AUDIT
 - *SECADM
 - *SERVICE
- A profile may be assigned to an individual user or to a group. Individuals may be members of a group - a good way to organize profiles.
- Some profiles are only for purposes of object ownership, and are not intended to provide system access

Object Authority

- Object Authority gives the access rights to an object
- Classed as either management or data authorities
- Primitive management Authorities are:
 - Operational
 - Management
 - Existence
 - Alter
 - Reference
- Primitive Data Authorities are:
 - Read
 - Add
 - Update
 - Delete
 - Execute

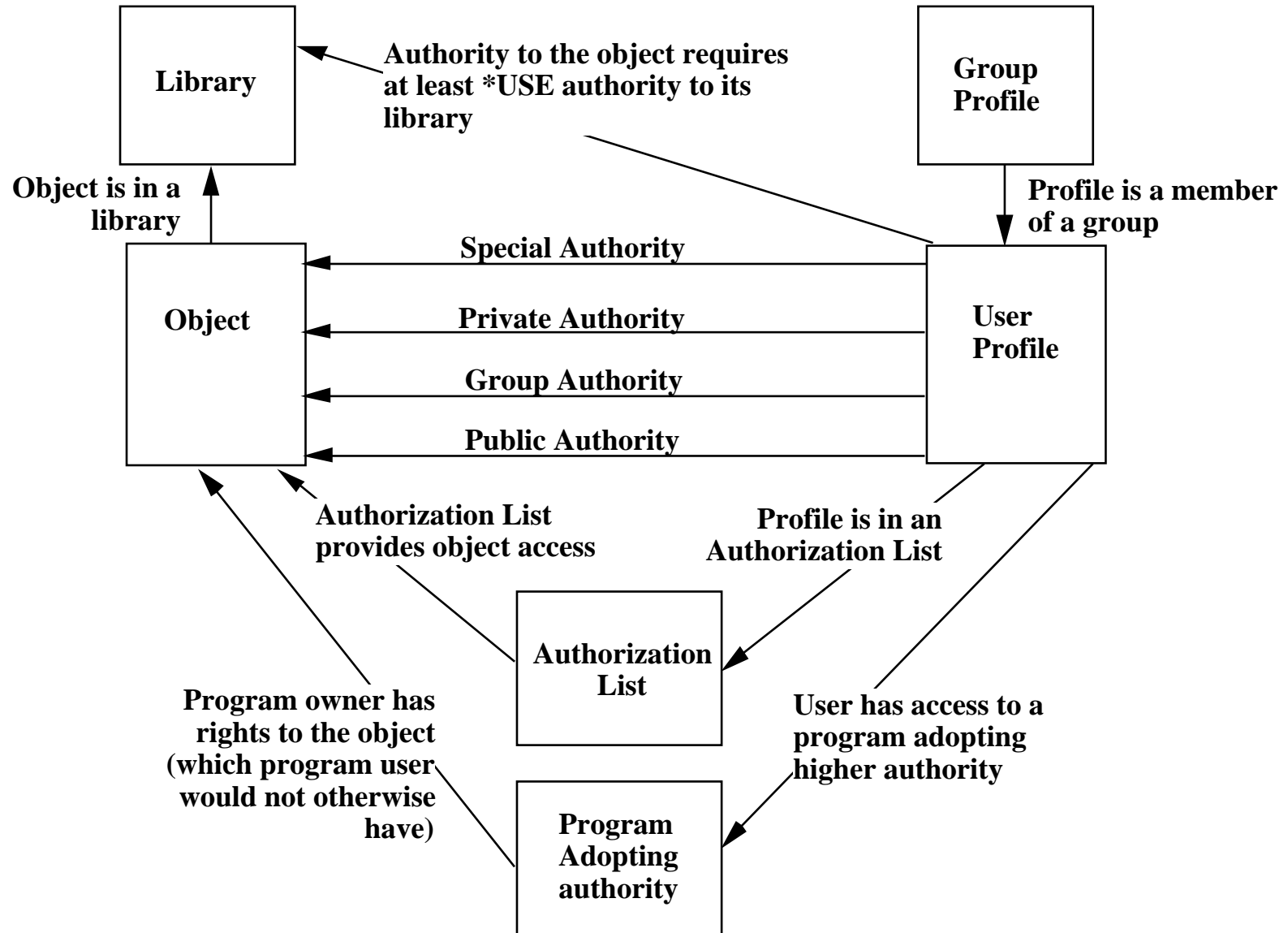
Object Authority

- Authorities may be combined in conventional ways:
 - *ALL
 - *CHANGE
 - *EXCLUDE
- Ways to assign authority to profile(s):
 - Private - to a specific user
 - Group - to a user through their membership in a group
 - Public - “and everyone else”; the authority to anyone not otherwise designated

Authorization Lists

- Feature carried over from S/36
- List of specific users having similar rights of set of objects
- Can change authority in “real time” - no object locking involved

The Security Model

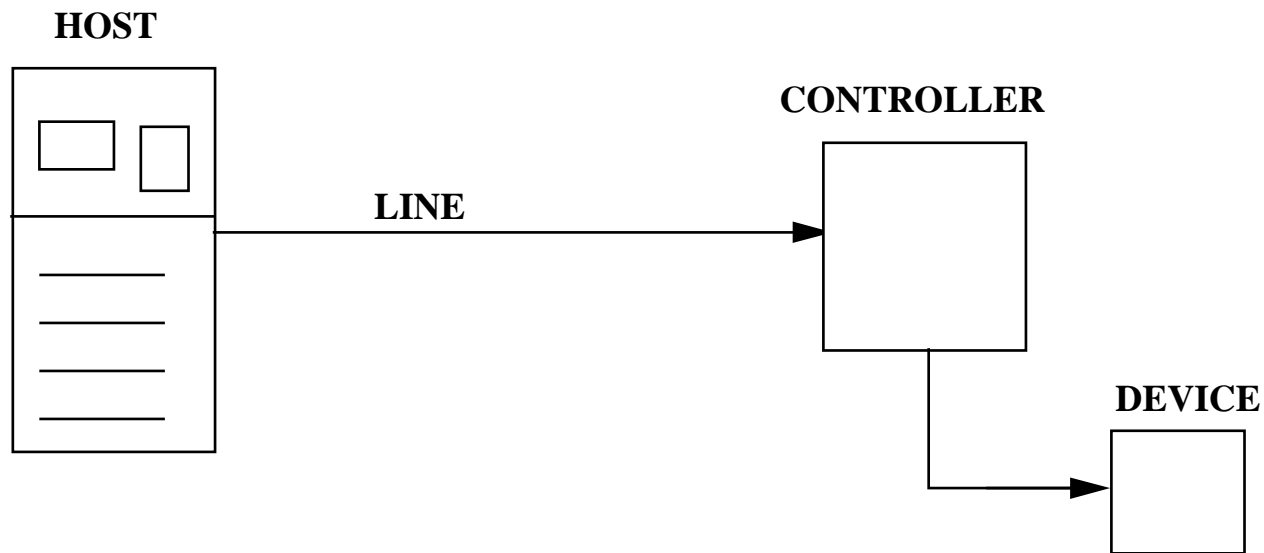


Application Security

- Implementation in an application environment
 - Library security
 - Program-enabled security
 - Application menus (with limited capability to keep users within the menus)

Communications Basics

- SNA derived, with emphasis on minicomputer environment
- APPN - Routing or network layer protocol
- APPC - Session/transport layer protocol
- Model is minicomputer with line, remote controller and remote devices:



- Model is applied to LAN-based configuration, TCP/IP, and all other communications

Communications Security

- Secure device objects
- Secure authority to change configuration
- Use Location Password for APPC communications
- Don't use Secure Location (= trusted remote system)
- Don't rely on menu security and limited capability
- Use outboard security devices when needed

Video - V3R1 Security Features

The AS/400 "Quick Audit" Commands

- DSPAUTUSR - Gets list of profiles
- DSSPUSRPRF - Detail information on specific profiles
- WRKSYSVAL - Display system values, note specific security values.

The AS/400 "Quick Audit" Fact Finding

- Compare active profiles to employment records to validate
- Review appropriateness of special authorities
- Ensure overall security level
- Password management
- Security Auditing enabled?

II. *Quick Audit Exercise*

1. Execute WRKSYSVAL. What are the values for the following? What are the security implications? (HINT: Press the “Help” key to get more information on each)

QSECURITY

QAUDCTL

QAUDLVL

QINACTV

QLMTDEVSSN

QLMTSECOFR

QMAXSIGN

QMAXSGNACN

QPWDMINLEN

QPWDEXPITV

QPWDRQDDIF

QPWDRQDDGT

QSYSLIBL

2. Execute DSPAUTUSR.

Are there profiles which do not appear associated with a specific, named user?

What are the group profiles on this system? Are all users associated with a group?

Do the group profiles have an active password?

Are there 'Q' profiles which are still active? Which ones?

II. Quick Audit Exercise, continued

3. For the active 'Q' profiles, execute the command DSPOBJD. Find out both the owner and the creator of these profiles. Have any of them NOT been created by IBM
4. Use DSPUSRPRF to find out the special authorities associated with:
 - QSECOFR
 - QPGMR
 - QSYSOPR

USING RAPPORT AUDITMASTER

- Obtaining and Loading the Software
- Login On
- The Report Menu
- Printing reports
- The Audit Program
- Level 1, 2, 3 Audits
- Review Categories
- “Gotchas” in AuditMaster
- Removing Auditmaster
- Missing from AuditMaster

Obtaining and Loading the Software

- Mary Sullivan in Montvale handles the master copies
- Frequent users should arrange an office resident copy
- Before you load Rapport, find out:
 - How many AS/400 machines you will be reviewing
 - Operating System versions
 - Type of tape drive (NOTE: May require media conversion)
- Basic load procedure:
 - Have client sign on as security officer
 - Place tape in drive and get name of drive from client (e.g., TAP01, TC, etc.)
 - Type:

```
RSTOBJ OBJ(INSTGR*) SAVLIB(RSAUDITMV2) DEV(name)
OBJTYPE(*ALL) RSTLIB(QTEMP)
```

and press enter
 - Type:

```
CALL QTEMP/INSTGR1 (name)
```

and press enter
 - Enter installation password when prompted

- When installation finishes, print the installation reports and sign off.
- Sign on as RSAUDITOR with password xxxxxxx, and change password when prompted

Loggin On

- Access restricted to menus - “audit safe”
- Requires separate sign-on
- User ID = RSAUDITOR

The Report Menu

- Only functions can be performed from menu
- All reports run in batch - minimizes performance impact
- Menu Tree:

Printing reports

- F6 - will show status of jobs. When in OUTQ status, reports are ready.
- F8 - will show all reports submitted
- To view a report:
 - Option 5 will display a report
 - Wxx in command line at top will "window" report to column xx
- To print a report:
 - Find out the output queue you should use. Get both the queue name and the library it is located (this is often QGPL).
 - Place a 2 in front of the report(s) you wish to print
 - Type outq(libxxx/queuexxx) in the bottom command line, where libxxx/queuexxx is the fully qualified print queue name.
- A spool file with a status of SAV has been printed at least once already. Once with a status of RDY has not yet been printed.

The Audit Program

■ Audit Steps

- Define business and information systems environment
- Define audit objectives
- Fact Finding - Rapport
- Fact Finding - Other (interviews, examination of procedures, etc.)

■ Organization of the Audit Program

- Sections A & B cover management and procedural issues.
- Sections C & D are more specific reviews of system configuration, requiring Rapport Auditmaster reports or their equivalent.
- Section E has “value added” reports, not necessary for controls but useful for the client.
- Appendix A has the report to menu items cross-reference of Auditmaster reports. Report R1, for example, is option 7 from the main menu, then option 3 from the next menu.
- Appendix B shows some alternatives to Auditmaster
- Appendix C is an outline of AS/400 security checking

The Audit Program

- Work Paper Considerations
 - Overview of Business and IS Environment
 - Specific Audit Steps - cross referenced to reports
 - Report Checklist - back of audit program
 - Other Fact Finding

Level 1, 2, 3 Audits

- Each level is a different level of scope
- Level 1
 - Emphasis on procedure verification
 - System wide password restrictions
 - Ensure profiles belong to active employees
 - Review powerful special authorities
- Level 2
 - Specific object security mechanisms
 - Verify specifics of procedures
 - Classification and proper authority granted user profiles
 - Object authority secures database update commands
- Level 3
 - Control system maintenance profiles
 - Detailed review of object authority and ownership
 - Object authority secures system management commands
 - Verify user library lists

Review Categories

- General Security
- User and Menu Settings
- Application and User Library Security
- Specific Object Security
- Network Security
- Device Security
- Change Control
- Security Monitoring and Reporting

“Gotchas” in AuditMaster

- Recommends level 30 security - should be level 40 or above
- File download reports generally “useless” (ref C5.3, C5.4)
- Currently does not encompass TCP/IP, IFS. etc., does not cover IOSYSCFG special authority, etc.
- User Assistance Level - not pertinent to controls
- User Class - more a housekeeping issue, only minimally impacts controls (C2.2.4, C2.2.8, etc.).
- Keep QCRTAUT at *CHANGE! (C3.1)
- Emphasis on library security assumes client follows this strategy - though other valid strategies exist
- Securing specific devices through object authority is rarely used - helpful for security, but not essential
- Audit program does not cover more technical system “hacks”
- Data classification, data ownership, records management policies may not be relevant to most AS/400 shops (A3.2, A3.3, and A3.5)

III. Exercise - AuditMaster Level 2 Audit

1. Log on to the AS/400 as the Rapport Auditmaster user RSAUDITOR.
2. Press F6. Are there any batch jobs displayed? If so, what state are they in? Are there any spool files associated with them?
3. Press F8. Are there any spool files associated with your session so far?
4. Review the items on the Rapport main menu.
5. Go to section C of your Audit “Programme”. Note that it requires report R1. To find which menu options are required to execute R1, refer to Appendix A of the Audit Programme.
6. Execute these reports. After submitting the report, go back to the main menu (F3), and from there press F6 to monitor the progress of your report.
7. When the report is finished (status = OUTQ), type the number 8 in front of the job, to view the spool files.
8. How many spool files are there? If there are two, one may be the actual joblog, the other the report itself. Type the number 5 in front of the report to view it.
9. Scroll forward to the end of the report. Note the value of QSECURITY as shown on the report.
10. Exit the report display. Type the number 2 in front of the spool file, and on the command line at the bottom of the screen, type OUTQ(*name*), where *name* is the name of the locally configured output queue.
11. Go to step C2.1.1 of the audit program. review the appropriate system values. What recommendations would you make with respect to these values on this system? How does the nature of system use (as an instructional system, rather than a financial/business transaction processing system) affect your findings?
12. What is report R3, required for audit steps C2.1.2 through C2.1.6? Which menu options must you go through to execute this report?

13. Execute report R3. Review the progress of the job through F6. When the report is completed, attempt to complete audit steps C2.1.2 through C2.1.6. What information would you need about this site's business environment to complete these questions (hint: It is something you might ask human resources)?

III. Exercise - AuditMaster Level 2 Audit, continued

14. Execute report R49. What are the group profiles on this system? How does this report compare with DSPAUTUSR in the “Quick Audit” exercise?
15. Execute report R7, to list some of the powerful profiles (based on their special authorities). How many profiles have *ALLOBJ authority? How many *SERVICE? *SECADM?
16. Go back to report R3, which you executed in step 13. Note the findings for audit step C2.2.5, by reviewing the last date these passwords have been changed. Do any of these profiles appear to still have their IBM-assigned profiles? How would you test these profiles to determine this with some certainty?
17. Execute reports R6 and R9. Review the initial menus and programs of the users. Do any of them look like application software menus? Do any of them look like AS/400 system menus? How could you tell?
18. Which users have limited capability *YES? Are these the same ones with initial menus for application software? What sort of user would have both limited capability *YES and an initial application software menu? What sort of user would have limited capability *NO and an initial AS/400 system menu? How would you make sure that users were corrected assigned the proper limited capability and menus?

Removing Auditmaster

- Delete all reports from Rapport output queues
- Delete libraries RSAUDITMV2 AND RSAUDITMVU
- Delete profile RSAUDITOR

Missing from AuditMaster:

- CHKOBJITG - report on object integrity, useful to see if programs have been patched
- Authority over device descriptions - guard against specifying bogus log-on screens
- Non-IBM commands in QSYS
- Report of programs adopting authority which execute security-problematic commands (call command entry, add libraries to library list)

The IBM Security Toolkit

- Additional no-cost software and very useful documentation at pre-V3R1
- Imbedded in operating system post V3R1
- Documentation is best concise description of AS/400 recommended security practices yet produced by IBM
- Software provides comprehensive set of reports, duplicating about 80% of Rapport Auditmaster
- Most of the audit program can be executed with Security Toolkit, if Auditmaster not available

The IBM Security Toolkit

Untitled-1: Slot:9Addr:1

SECBATCH **Submit or Schedule Security Reports To Batch** System: S1010716

Select one of the following:

Submit Reports to Batch

1. Adopted object information
2. Audit record report
3. Authorization list authorities
4. Command authority
5. Communications information
6. Document authority
7. File authority
8. Folder authority
9. Job description authority
10. Library authority
11. Object authority
12. Private authority
13. Program authority

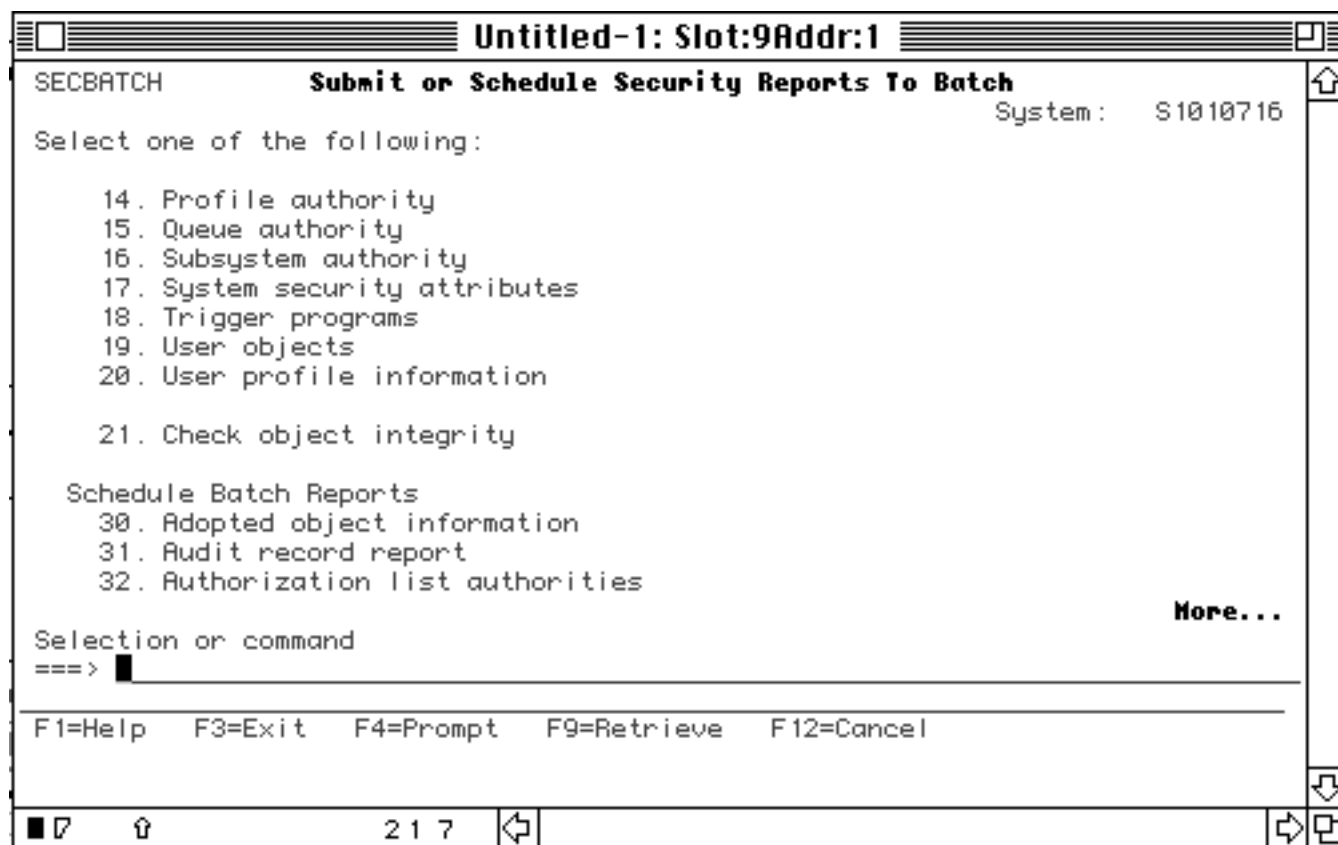
More...

Selection or command
===> _____

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

2 1 7

The IBM Security Toolkit



IV. Security Toolkit Exercise

ADVANCED TOPICS

- TCP/IP
- ODBC and LAN connectivity issues
- Hackers
- Cryptography & the AS/400
- Auditing J.D. Edwards

TCP/IP

- New to AS/400, hence lack of familiarity
- Voids “Limit Capability” and menu security

ODBC and LAN connectivity issues

- Voids “Limit Capability” and menu security
- User friendly ODBC-based software particular threat
- Object authority “catch 22”
- End user access to system objects
- Remedies:
 - Exit programs
 - Application granted object access

Hackers

- More typically technically sophisticated insiders
- Typical hacker relies on application-level “tricks”
 - “Hidden” user profile with high authority
 - “Hidden” program which adopts high level of authority
 - Password capture program
- Operating system compromises are possible, though rare.
- To minimize:
 - Restrict ability to restore software or objects onto system
 - Restrict and audit use of system service tools
 - Document and audit programs which perform system functions

Cryptography & the AS/400

- IBM Products:
 - Cryptographic Services/400 - Software only
 - Common Cryptographic Architecture Services/400 (CCAS/400) - Software & hardware
 - LU6.2 Session Level Encryption
- Prime Factors DESCRYPT +, EDICRYPT + (Now owned by Premenos)
- PGP
- Primarily Banking Applications
- Little current use of public key technology

Auditing J.D. Edwards

- Most common AS/400-based financial package
- The J.D. Edwards application software includes certain configuration values and tables which affect security and user access. These parameters include the following:
 - Action Codes, which determine specific programs to which a user has access, and whether this access includes change, add, or delete rights to data.
 - Cost Center Codes, which facilitate assigning access levels to organizational units.
 - Menu Masking, which secure entire or individual menus on a menu for each user.
 - Function Key Security, which secure function keys by video screen or user.
 - Batch Approval/Post Security, which restricts unauthorized postings of batch transactions by users.

Auditing J.D. Edwards

- Users of J.D. Edwards are initially configured according to the *GLOBAL group profile.
- Fast-path allows users to “jump” to different menus by entering the menu ID
- The A901 menu in JDE includes the Selection History Log option. This function allows a JDE administrator to review the specific functions a user has executed, the menu selection, date, job number, and job executed.

USING THE LOS ANGELES AS/400 SYSTEM

X. Exercise - Installing and login into the Los Angeles AS/400

Appendix A. - Auditmaster reports required for Audit Program

Prog ref	Report ref	Menu	Report name
R1.	AUDSVLRP	7,3	Security systems value report
R2.	QSYSPRT	7,4	Report on all system values
R3.	AUDPRFSG	6,2	User password/sign-on report
R4.	AUDDRMUS	6,4	Dormant user report
R5.	AUDDSAPF	6,7,1	User profiles with status disabled
R6.	AUDPRFIP	6,3	User profile initial program report
R7.	AUDSPCPF	6,7,3	Users with *ALLOBJ or *SERVICE special authority
R8.	AUDUSAUT	6,1	User authority control report
R9.	AUDLMTPF	6,7,2	Users with limit capability *NO or *PARTIAL
R10.	AUDJRNSD	9,6,3	Changes of DST security officer password
R11.	AUDLIAUT	1,1	Library authorities control report
R12.	AUDLIAUP	1,2	Library *PUBLIC authorities control report
R13.	AUDAUTLS	1,9	Authorisation list user/object report
R14.	AUDCMDAU	8,3	Command authority report
R15.	AUDPGMAD	5,1	Program authority adoption
R16.	AUDJBDAD	5,2	Job description authority adoption
R17.	AUDSBSRP	5,3	Subsystems with WSE entry
R18.	AUDDEVAU	4,1	Workstation authorities report
R19.	AUDEVALL	4,2	Workstation *ALLOBJ authorities report
R20.	QSYSPRT	10,2	Display network security attributes
R21.	AUDPCSRP	10,1,1	File transfers between PC and IBM AS/400
R22.	QSYSPRT	10,3	Display directory entries
R23.	AUDOUTQS	12,4	Output queue security settings
R24.	AUDSGNON	2,1	Invalid sign-on attempts report
R25.	AUDAUTHR	2,3	Attempts to use objects without authority
R26.	AUDEDESCR	2,4	Changes to device, job and subsystem.
R27.	AUDLGINT	2,9	History log file integrity report

Appendix A. - Auditmaster reports required for Audit Program (continued)

Prog ref	Report ref	Menu	Report name
R28.	AUDJRNAF	9,1	Attempts to use objects without authority
R29.	AUDJRNPW	9,2	Invalid sign-on attempts
R30.	AUDJRNRU	9,3,3	Restores of user profiles
R31.	AUDJRNCA	9,6,1	Changes to object authority
R31.	AUDJRNOW	9,6,1	Changes to object ownership
R32.	AUDJRNCP	9,6,2	Changes to user profiles
R33.	AUDJRND0	9,4	Deletions of objects
R34.	AUDJRNNA	9,6,5	Changes to network attributes
R35.	AUDJRNJD	9,6,4	Changes to job description user parameter
R35.	AUDJRNPA	9,6,4	Changes to program authority adoption
R36.	AUDJRNSV	9,6,7	Changes to system values
R37.	AUDJRNRP	9,3,2	Restores of programs adopting authority
R38.	AUDJRNCO	9,5	Creations of new objects
R39.	AUDJRNRO	9,3,1	Restores of objects with changed ownership
R40.	AUDJRNSE	9,6,6	Changes to subsystem routing entries
R41.	AUDNEWOB	1,8,1	New objects report
R42.	AUDRSTOB	1,8,2	Library restored objects report
R43.	AUDSYSVL	2,2	Changes to system values report
R44.	AUDUNSAV	1,8,3	Unsaved objects report
R45.	AUDUNPGM	1,8,4	Unused programs report
R46.	AUDRGFIL	1,8,5	Files needing reorganisation report
R47.	AUDOBJAU	1,8,6	Object authority verification report
R48.	AUDLIBDC	1,5	Library size/description report
R49.	QSYSPRT	6,6	List of all user profiles by group
R50.	QSYSPRT	App B	Library list (*LIBL) for a user
R51.	QSYSPRT	App B	Systems value report
R52.	QSYSPRT	App B	List of user profiles
R53.	QSYSPRT	App B	List of authorised users

Appendix A. - Auditmaster reports required for Audit Program (continued)

Prog ref	Report ref	Menu	Report name
R54.	AUDLIOBJ	1,3	Objects changed in libraries report
R55.	AUDCMDAC	3,2	User command usage report (daily only)
R56.	AUDLIACH	1,4	Library authorities/ownership change report
R57.	AUDSVRST	2,5	Saves to tape or disk
R58.	AUDSECMS	2,6	History log security message report
R59.	AUDSECHL	2,7	Specific history log message report
R60.	AUDUSRAC	3,1	User activity report