ISACA Annual Conference
August 24, 2008

Operating Systems Security

OS 400

Santosh Satam
Head – Technical Services

Agenda

- AS/400 Primer
- Operating System Security – OS/400
- Case Study
- Resources for AS/400 Audit
- Q&A

System-i Evolution

- Server
  - AS/400™ (1988 – 1998)
  - iSeries™ (1998 – 2004)
  - i5™ (2004 – 2006)
  - System i™ (2006)
- Operating System
  - OS/400 (1993 – 2004)
  - i5/OS ™ (2004)

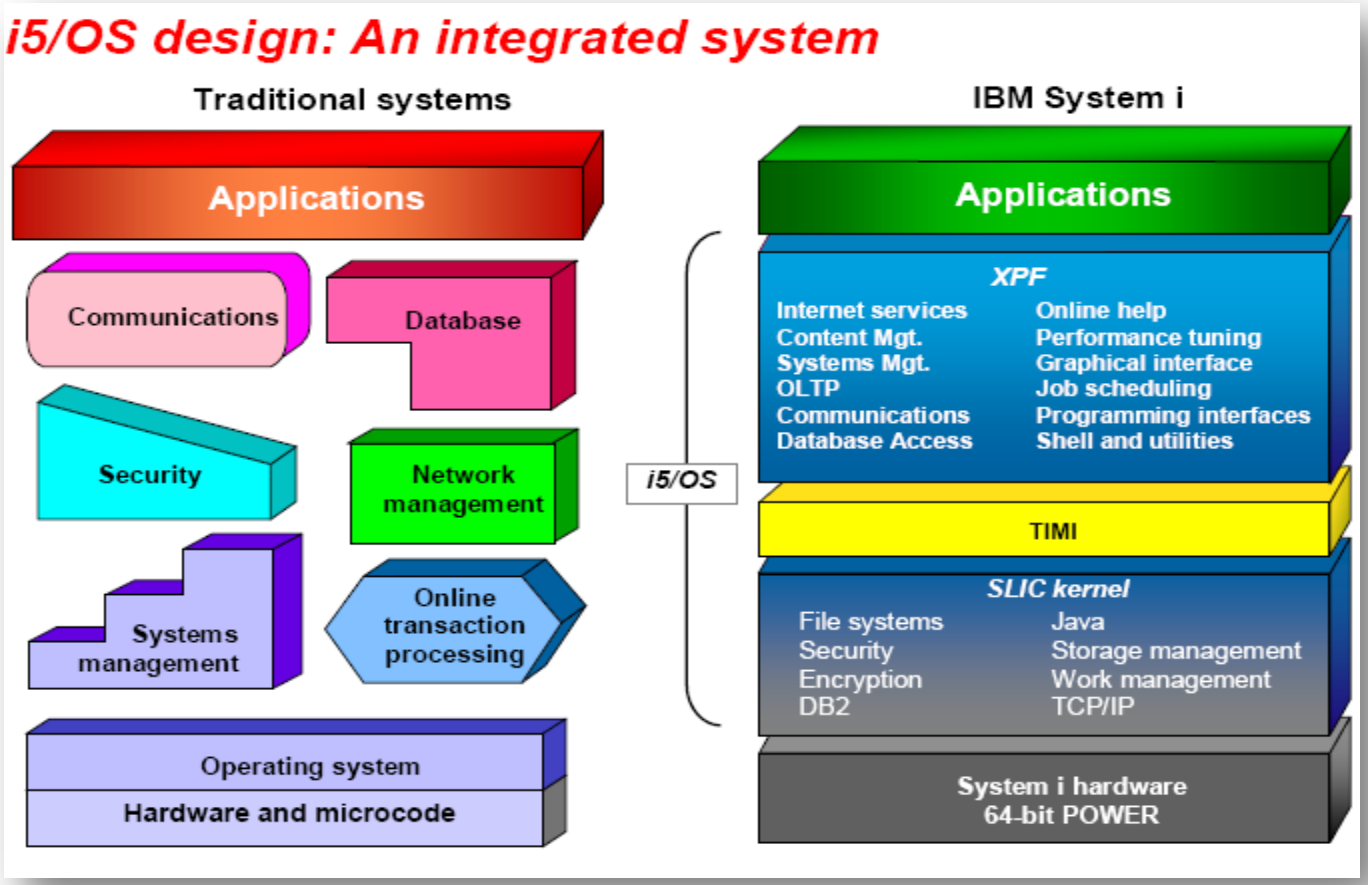
System-i Market

- 98% of Fortune100 run System i
  - Source: IBM
- 400,000 systems installed worldwide
  - 45% US, 35% Europe with 20% Asia
- 30,000 new systems ship annually
  - Price range from $12,000 to $1 million +
- 16,000 banks run on the System i

What is an AS/400 ?

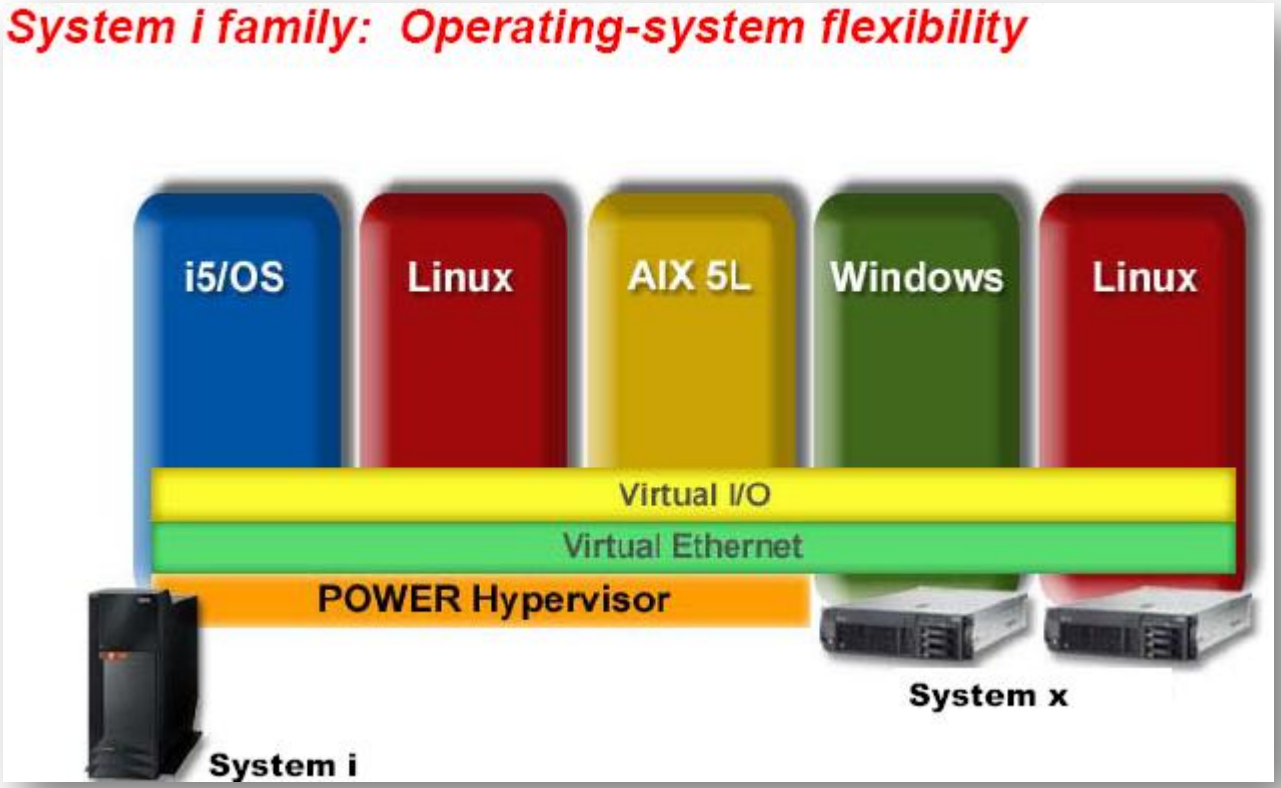
- Successor to the former S/36 and S/38 midrange computers
- AS/400 is an object-oriented system
- Everything related to the AS/400 platform is considered an object, programs, files, printers, users and databases all are objects.
- Security is built-in, it's not a separate product
- First general-purpose computer system to attain a C2 security rating from the NSA
- It runs of POWER5 processor.

I5/OS - Design

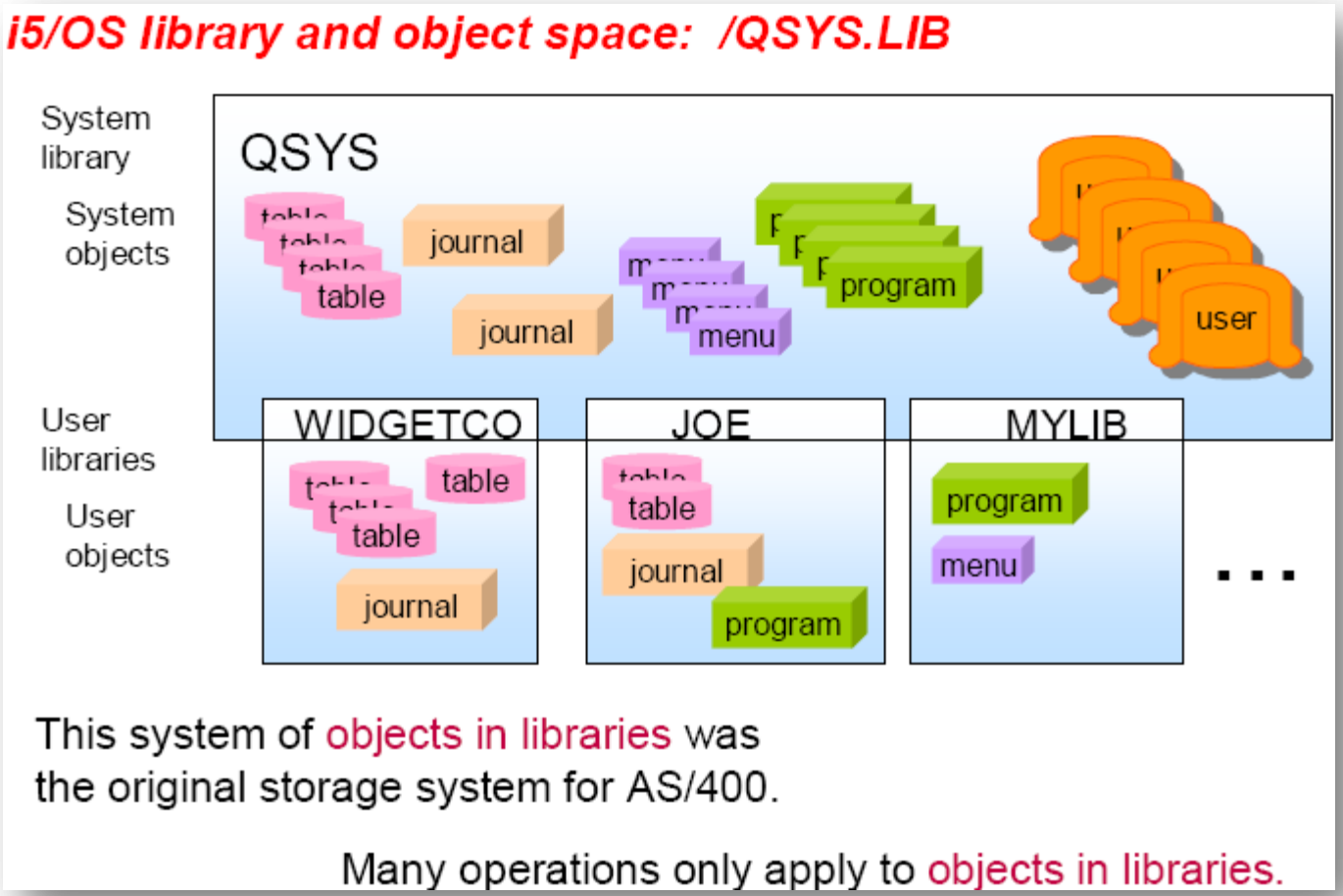


TIMI - Technology Independent Machine Interface

Operation System- Flexibility



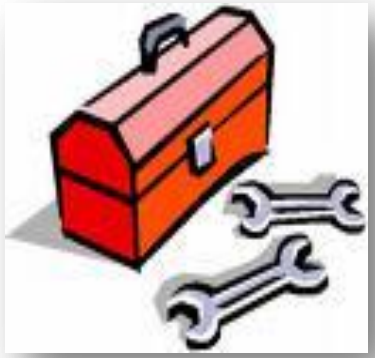
I5/OS – Library and Object space



What to Look for ?

- Network access
- Program, file and library security
- User security
- System Authorities
- System Security
- Auditing and Logging

Auditor's Toolbox



TOOLBOX

- Background information on AS/400
- Access to an AS/400 security administrator
- Built-in Security Tools

Auditor's Toolbox – Security Tools

- User Security Tools
  - Find out what user profiles have default passwords.
  - Schedule user profiles to be unavailable at certain times of the day or week.
  - Schedule a user profile to be removed when the employee leaves
  - Find out which user profiles have special authorities.
  - Find out which user profiles having invalid sign-on attempts.
- System Security Tools
  - Compare the settings on your system to the recommended settings.

Network Access

- IBM introduced a TCP/IP with version 3.1 of OS/400 in 1994.
- OS/400 ships with all TCP/IP services active by default
- Users can use simple tools such as FTP or ODBC to download or upload data between their personal computing devices and System-i.
- Users who can change or delete data + Open servers like FTP and ODBC = Disaster
- IBM introduced exit points for various TCP/IP Servers but did not provide exit programs.

Network Access

- List of exit points where risk of exposure is high

Exit Point Server	Description
*DDM	Alternate ODBC Server
*DQSRV	Client Data Queue Server
*FILESRV	Remote File Server
*FTPCLIENT	TCP/IP Outbound File Transfer
*FTPSERVER	TCP/IP Inbound File Transfer
*NDB	ODBC & JDBC Native Database
*RMTSRV	Remote Command Server
*RTVOBJINF	ODBC & JDBC Retrieve Object Info
*SQL	ODBC & JDBC Signon
*SQLSRV 1	ODBC & JDBC Server
*SQLSRV 2	ODBC & JDBC Server
*TELNET	TCP/IP Terminal Emulation

Network Access

- How to determine the existence of Exit Programs
  - WRKREGINF
- What information you get:
  - User JOE connected to system XYZ from remote IP, address 196.6.3.104 at 10:22 a.m. At 10:24 a.m., he sent a request to download the Payroll file, and at 10:31 a.m., he ran a remote command that attempted to delete his joblog.
- What should be monitored and Controlled:
  - Services such as FTP, remote command and remote SQL
  - Sys admin should maintain logs of exit point traffic, and review the access rules that control the exit programs.

Program, file and library security

- OS/400 paths come in two basic flavors, Traditional Unix paths, and OS/400 libraries
- It is not unusual that the public has rights to add objects to where the operating system lives (Library QSYS)
- Libraries where the user has *CHANGE rights (or better) are a serious exposure
- OS/400 objects (files, programs, etc.) are for everyone (*PUBLIC) to have at least change (*CHANGE) rights to all parts of an application.
- This allows users add or delete entries in the file and to change some of the external properties of a file. (like rwx in Unix)

Program, file and library security

- How to object authority, to see whether a particular system allows too much authority to important application objects
  - DSPOBJAUT OBJ(Library_Name /File_Name) OBJTYPE(*FILE)
  - DSPOBJAUT OBJ(QSYS/library name) OBJTYPE(*LIB)

- What should be monitored and Controlled:
  - Every significant production database, production libraries and source code

User Security

- User security is critical as they are the most obvious, and the most exploited, method of compromising a system.
- By default, System-i assigns to new user profiles a default password that is the same as the username.
- Un-monitored user IDs are the easiest way to get into any system
- On OS/400, there is no way to force a special character without writing custom code in a password validation exit program.

User Security

- How to check the system values specific to password Settings:
  - System Values DSPSYSVAL SYSVAL(QPWD*)
  - Users with default passwords ANZDFTPWD ACTION(*NONE)
  - Inactive users (DSPUSRPRF USRPRF(*ALL))
- What should be monitored and Controlled
  - System parameters which determines password expiry period, minimum length of the password, password must be different from previous etc.
  - Powerful users who have default passwords
  - Users who have not used system more than 30 days
  - Invalid Sign on attempts

System Authorities

- There are eight types of administrative rights delivered by IBM

Authority Name	Special Authority Description
*ALLOBJ	Root- or administrator-level access (very powerful)
*SECADM	Security administrator (can create new user profiles)
*IOSYSCFG	Network services configuration
*AUDIT	Configuration of audit and logging settings
*SPLCTL	Full access to reports and printer spool files
*SERVICE	Hardware administration
*JOBCTL	System operator controls
*SAVSYS	Backup and restore operations

- The most important of these special authorities is *ALLOBJ
- Special authorities tend to be handed out liberally

System Authorities

- How to check for powerful administrative privileges password Settings:
  - Display User profile (DSPUSRPRF USRPRF(*ALL))
- What should be monitored and Controlled
  - Work to remove the administrate rights from most users, and continuously monitor these rights

System Security

- OS/400 provides a variety of methods of securing both the operating system itself, and the workstations that are connected to it.
- System values are the foundation of a secure system.
- System values define things like default public authority, default paths, base security level, audit levels, etc.
- Most important of the system values is QSECURITY which defines the overall security level of the operating system itself

System Security

- How to check for system values:
  - Security related system values (DSPSYSVAL *SEC)
- What should be monitored and Controlled
  - IBM recommends that all systems should be set to security level 40 or higher, and all new systems ship with a default value of 40.
  - Should be verified on a regular basis

Auditing and Logging

- The System Security Audit Journal (QAUDJRN) holds security related event log data
- The audit journal is a free feature of i5/OS, but it must be turned on and properly configured in order to do its job.
- Important Audit Value

Audit Value	Description	Importance
*AUTFAIL	Log Authority failures	High
*DELETE	Log deletion of objects	High
*OBJMGT	Log object management changes	High
*SYSMGT	Log changes to certain system management areas	High
*SAVRST	Log restore actions to security sensitive objects	High
*SECURITY	Log security related changes	High
*SERVICE	Log usage of the system and hardware service tools	High
*PGMFAIL	Log Program failures caused by security violations	High

Auditing and Logging

- How to check for system values:
  - Check the system value QAUDCTL which specifies what type of auditing is allowed on the system.
  - Check the system value QAUDLVL which specifies what types of security events should be audited.
- What should be monitored and Controlled
  - It is most practical to conduct regular reviews using a reporting tool since the format of the audit journal makes it difficult to read.

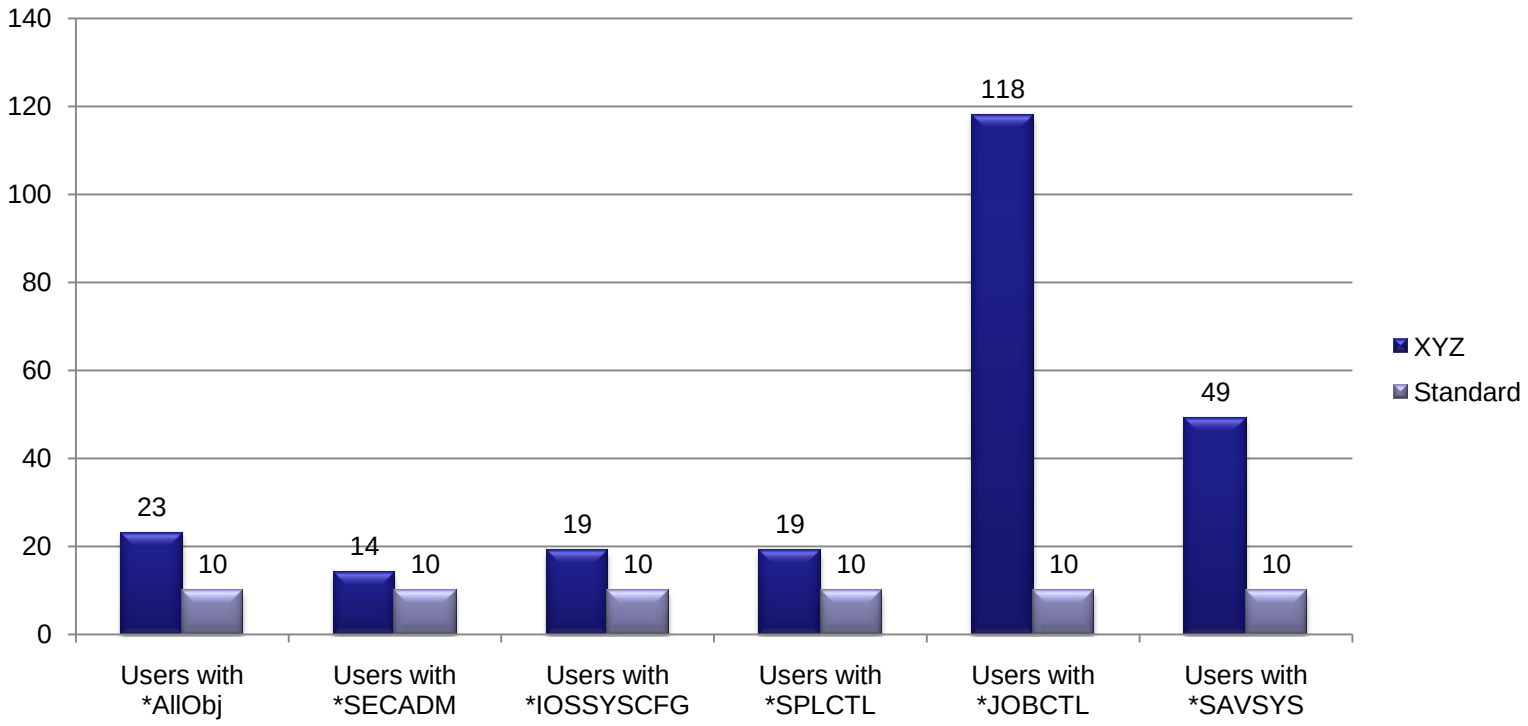
Case Study – AS/400 Technical Audit

Company: XYZ, one of the Largest Insurance Company in a SAARC Region
No. Of Users: ~ 1000
Hardware: AS/400 Model i520
OS: i5OS - v5r3

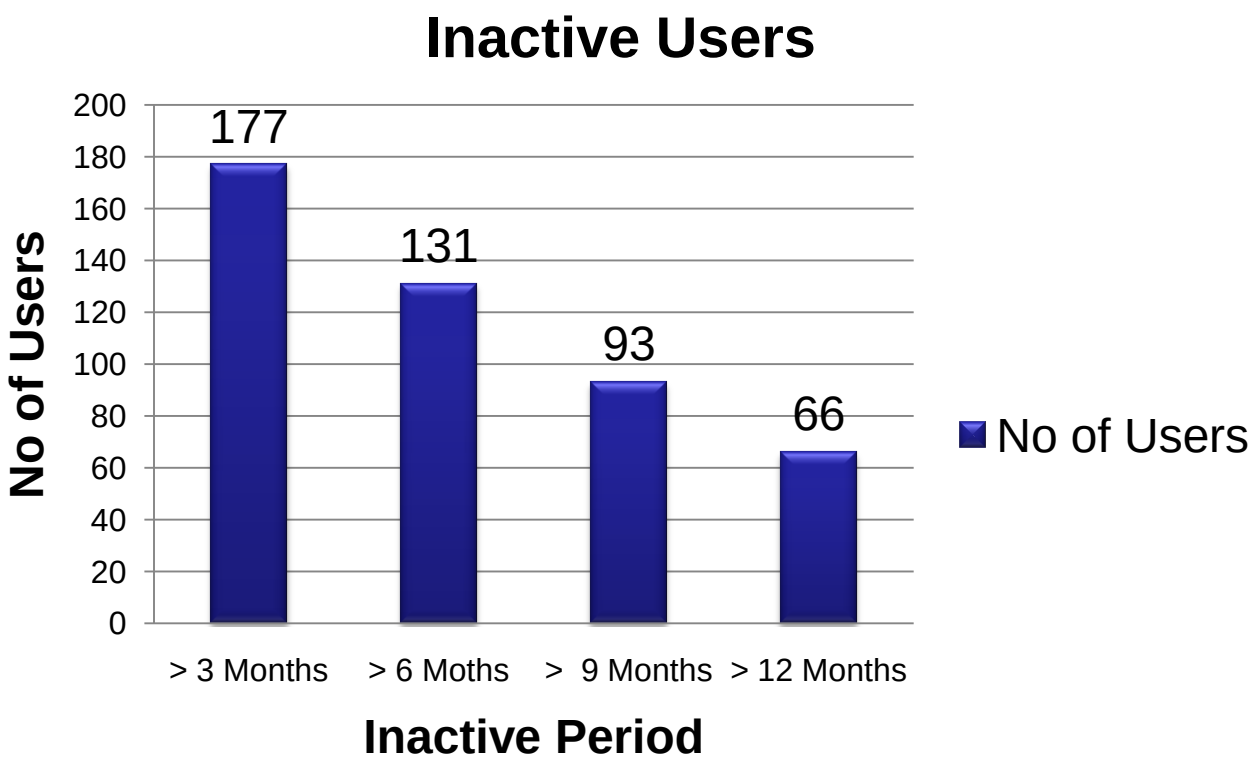
Application: Core Insurance (Life and General) Applications, Finance Accounting system, Document Archival & Retrieval System
Database : DB2

Network Access	
Prog, File and Library Security	
User Security	
System Authorities	
System Security	
Auditing & Logging	

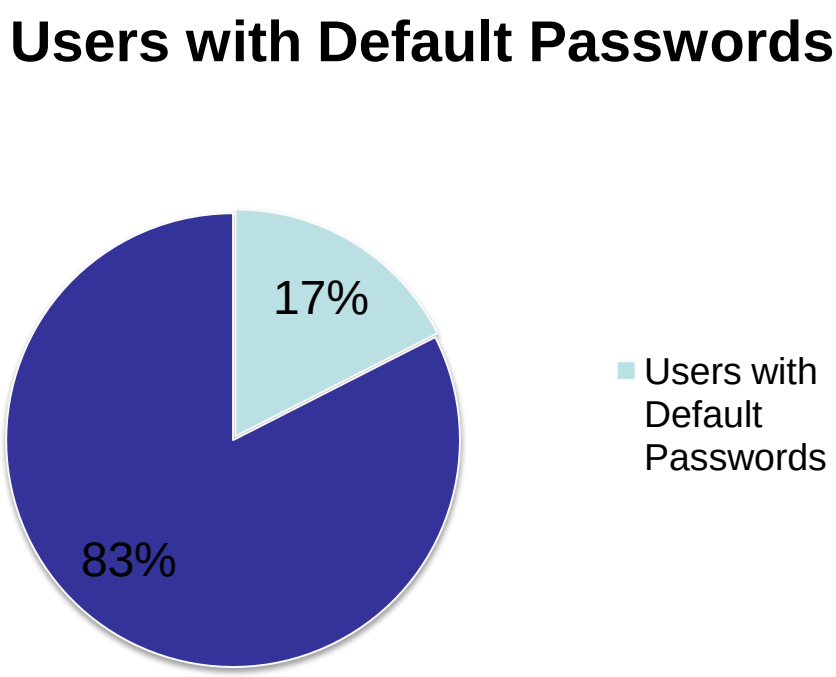
System Authorities



Inactive Users



Users with default password



System Security

Parameter	Current Value	Recommended	Comments
QPWDRQDDIF	0	1	Password reuse cycle
QLMTDEVSSN	0	1	There is no limit to the number of concurrent sessions a user can
QDSPSGNINF	0	1	Display sign-on information
QINACTITV	*NONE	60	Inactive Job Timeout
QLMTSECOFR	0	1	security officer can sign on to any workstation.

Auditing and Logging

Audit Value	Description	System Value	Importance
*AUTFAIL	Log Authority failures	NO	High
*DELETE	Log deletion of objects	YES	High
*OBJMGT	Log object management changes	YES	High
*SYSMGT	Log changes to certain system management areas	NO	High
*SAVRST	Log restore actions to security sensitive objects	YES	High
*SECURITY	Log security related changes	YES	High
*SERVICE	Log usage of the system and hardware service tools	NO	High
*PGMFAIL	Log Program failures caused by security violations	YES	High
*CREATE	Log creation of new objects	YES	Medium
*JOBDTA	Log job events such as start and stop.	NO	Medium
*PGMADP	Log usage of programs that adopt authority	NO	Medium
*NETCMN	Log APPN firewall events	NO	Low
*OFCSRV	Log Office Vision/400 security changes	NO	Low
*OPTICAL	Log usage of optical storage devices	NO	Low
*PRTDTA	Log printing functions	YES	Low
*SPLFDTA	Log usage of spooled files (reports)	YES	Low

References

- IBM-AS/400 Advanced Series: Tips and Tools for Securing Your AS/400 [SC41-5300-03]
- Fortress Rochester: The Inside Story of the IBM Iseries By Frank G. Soltis
- Auditor Resource Site: www.audit400.com
- Auditing IBM AS/400 and System i By John Earl (ISACA -Journal Online)
- iSeries Security Reference Version 5 [SC41-5302-07]
- www.isaca.org
- www.ibm.com

Conclusion

- IBM System i is a powerful business platform, but data are secure only if the IT department configures the system correctly and maintains adequate controls over the management of the system and its applications.

Q&A

Santosh Satam
ssatam@mielesecurity.com