
The State of System i Security & The Top 10 OS/400 Security Risks



Agenda

- **Introduction**
- **The Top Ten**
 - » **Unprotected Network Access**
 - » **Powerful Users**
 - » **Weak or Compromised Passwords**
 - » **User Identity Theft**
 - » **The Open Door Policy**
 - » **Promiscuous Object Ownership**
 - » **Library and Library List Problems**
 - » **Command Interface Abuse**
 - » **System Value Weaknesses**
 - » **No Audit Ability**
- **Conclusion**

The State of iSeries Security- 2006

- **188 Companies - Mostly in the US**
- **195 Different iSeries Systems**
- **825 users on average**
- **393 libraries on average**

Purpose of the Study

- **Help IT managers and auditors understand iSeries security exposures**
- **Focus on top areas of concern in meeting regulatory compliance**

What Drives Compliance

- **Security has increased in visibility and importance**
- **Companies are getting skewered in the press**
 - » **Bank of America, Marriott, Citibank, ChoicePoint, etc.**
- **The general public is concerned for it's safety**

The Legislature Reacts

- **Legislatures create laws**
 - » Sarbanes Oxley, HIPAA, Gramm-Leach-Bliley, SB1386, etc.
- **Laws are open to interpretation**
 - » **Sarbanes Oxley Section 404 –**
 - “Perform annual assessment of the effectiveness of internal control over financial reporting...”
 - “...and obtain attestation from external auditors”
- **Auditors are the interpreters**

The Auditor's View

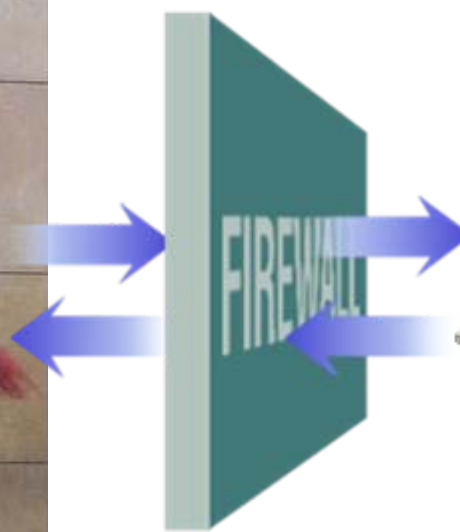
- **Auditors interpret regulations**
 - » **Auditors focus on frameworks and processes**
 - » **Auditors have concluded that IT is lagging when it comes to internal controls**
- **Executives just follow the auditors recommendations**
- **So what are the auditors going to say when they review your systems?**

The Biggest Threat to Your Data

HACKERS!!!

or

Your Company



Unprotected Network Access



- **Many OS/400 applications rely on menu security**
 - » It was easy to build
 - » It's the 'legacy' of business applications
- **Most menu 'security' designs assume:**
 - » *All* access is through the application menu
 - » No users have command line access
 - » Query access is limited or denied completely
 - » That the *user is a member of the group* that owns the objects. Or...
 - » *PUBLIC has broad access to the data

Result: Too Much Access



ODBC

XYZ Corporation CORPORATE PAYROLL									
Emp ID	Emp Name	Emp Title	Emp Salary	Emp Hire Date	Emp Dept	Emp Status	Emp Location	Emp Manager	Emp Supervisor
1001	John Doe	Software Engineer	75000	2008-01-15	Engineering	Active	New York	1002	1003
1002	Jane Smith	Product Manager	85000	2007-03-20	Marketing	Active	New York	1004	1005
1003	Bob Johnson	Sales Representative	60000	2009-05-10	Sales	Active	Chicago	1006	1007
1004	Alice Brown	Human Resources	55000	2006-11-01	HR	Active	New York	1008	1009
1005	Charlie Davis	Operations Manager	70000	2008-08-05	Operations	Active	Los Angeles	1010	1011
1006	Diana Prince	Marketing Specialist	65000	2009-02-18	Marketing	Active	New York	1002	1012
1007	Frank Miller	Software Engineer	75000	2008-04-22	Engineering	Active	New York	1002	1013
1008	Grace Wilson	Human Resources	55000	2006-11-01	HR	Active	New York	1008	1014
1009	Henry Taylor	Operations Manager	70000	2008-08-05	Operations	Active	Los Angeles	1010	1015
1010	Ivy Anderson	Marketing Specialist	65000	2009-02-18	Marketing	Active	New York	1002	1016
1011	Jack Thomas	Software Engineer	75000	2008-04-22	Engineering	Active	New York	1002	1017
1012	Karen White	Marketing Specialist	65000	2009-02-18	Marketing	Active	New York	1002	1018
1013	Liam Garcia	Software Engineer	75000	2008-04-22	Engineering	Active	New York	1002	1019
1014	Mia Martinez	Human Resources	55000	2006-11-01	HR	Active	New York	1008	1020
1015	Noah Hernandez	Operations Manager	70000	2008-08-05	Operations	Active	Los Angeles	1010	1021
1016	Olivia Lopez	Marketing Specialist	65000	2009-02-18	Marketing	Active	New York	1002	1022
1017	Peter King	Software Engineer	75000	2008-04-22	Engineering	Active	New York	1002	1023
1018	Quinn Scott	Marketing Specialist	65000	2009-02-18	Marketing	Active	New York	1002	1024
1019	Ryan Adams	Software Engineer	75000	2008-04-22	Engineering	Active	New York	1002	1025
1020	Sarah Baker	Human Resources	55000	2006-11-01	HR	Active	New York	1008	1026
1021	Timothy Clark	Operations Manager	70000	2008-08-05	Operations	Active	Los Angeles	1010	1027
1022	Uma Evans	Marketing Specialist	65000	2009-02-18	Marketing	Active	New York	1002	1028
1023	Victor Foster	Software Engineer	75000	2008-04-22	Engineering	Active	New York	1002	1029
1024	Wendy Green	Marketing Specialist	65000	2009-02-18	Marketing	Active	New York	1002	1030
1025	Xavier Hill	Software Engineer	75000	2008-04-22	Engineering	Active	New York	1002	1031
1026	Yara King	Human Resources	55000	2006-11-01	HR	Active	New York	1008	1032
1027	Zoe Lee	Operations Manager	70000	2008-08-05	Operations	Active	Los Angeles	1010	1033
1028	Adam Scott	Marketing Specialist	65000	2009-02-18	Marketing	Active	New York	1002	1034
1029	Benjamin Taylor	Software Engineer	75000	2008-04-22	Engineering	Active	New York	1002	1035
1030	Chloe White	Marketing Specialist	65000	2009-02-18	Marketing	Active	New York	1002	1036



Application Menu CRM



Telnet

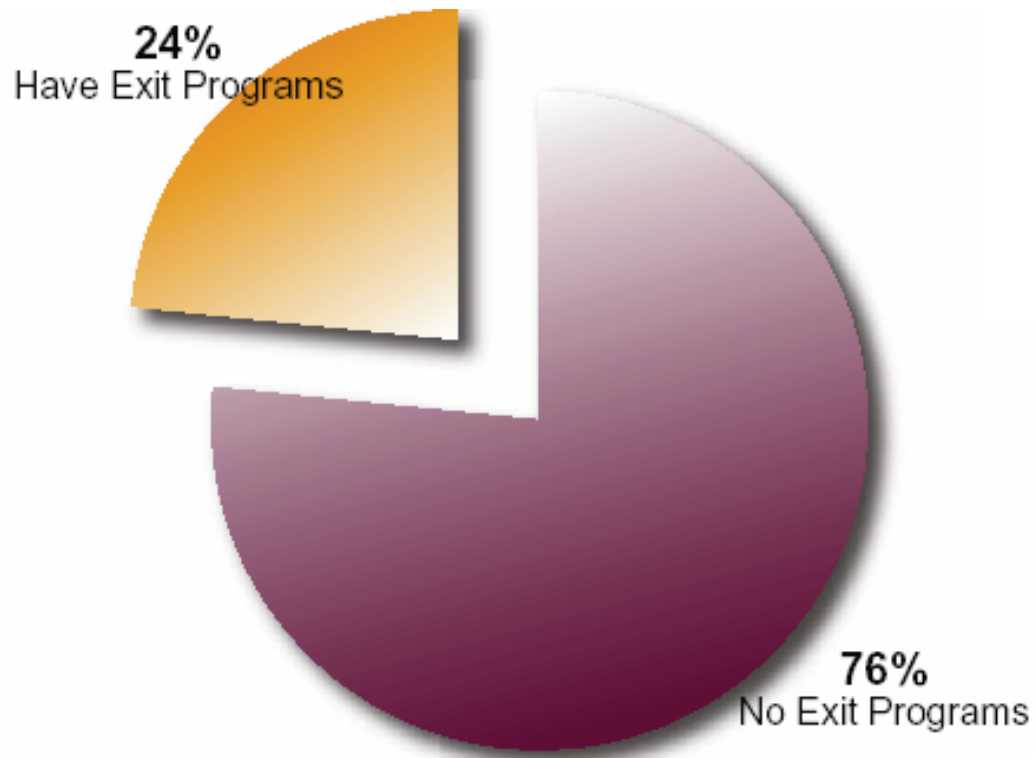
Unprotected Network Access



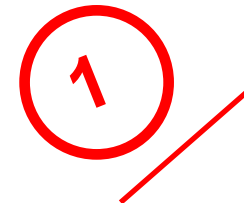
```
C:\WINDOWS\system32\cmd.exe - ftp westpt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\john.earl>ftp westpt
Connected to westpt.powertech.com.
220-QTCP at WESTPT.POWERTECH.COM.
220 Connection will close if idle more than 15 minutes.
User (westpt.powertech.com:(none)): john
331 Enter password.
Password:
230 JOHN logged on.....
ftp> put c:\junk.txt john/customer
200 PORT subcommand request successful.
150 Sending file to member CUSTOMER in file CUSTOMER in library JOHN.
250 File transfer completed successfully.
ftp: 4567 bytes sent in 0.02Seconds 228.35Kbytes/sec.
ftp>
```

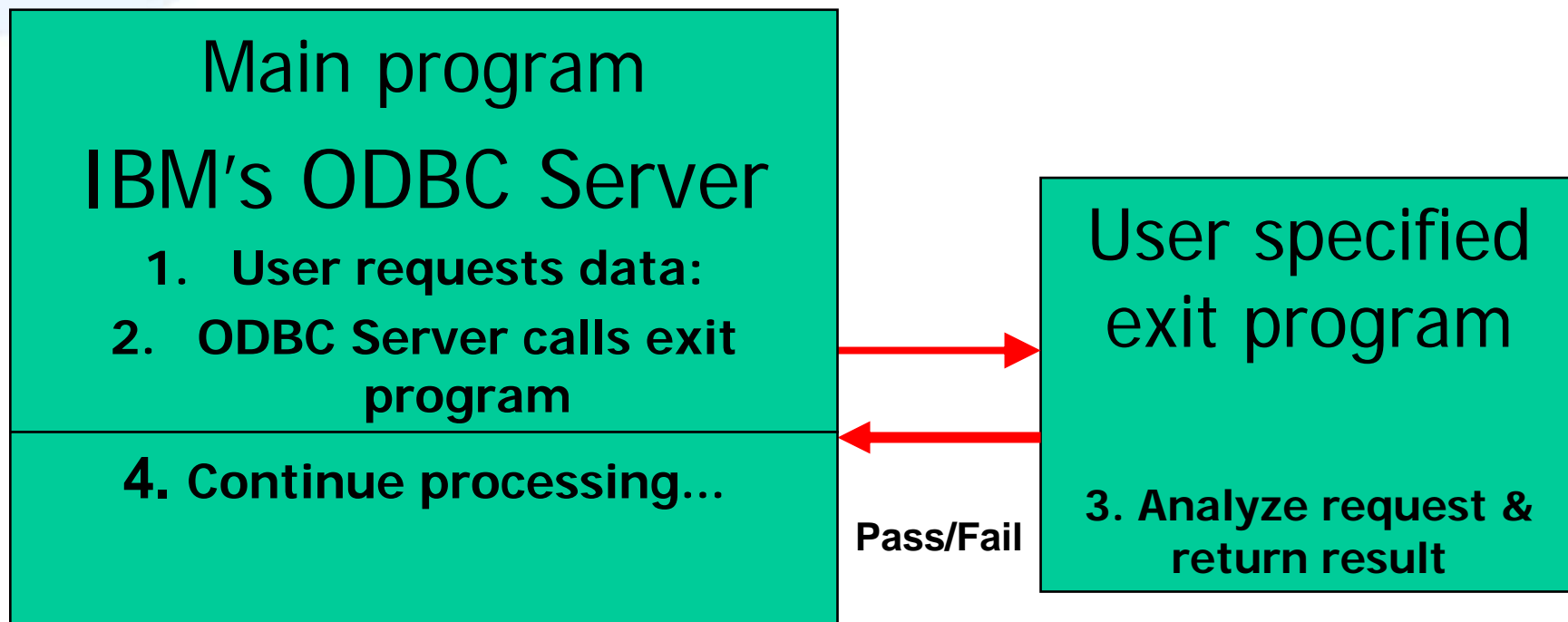
Actual State of iSeries Network Access Control



Unprotected Network Access



What is an exit point anyway?

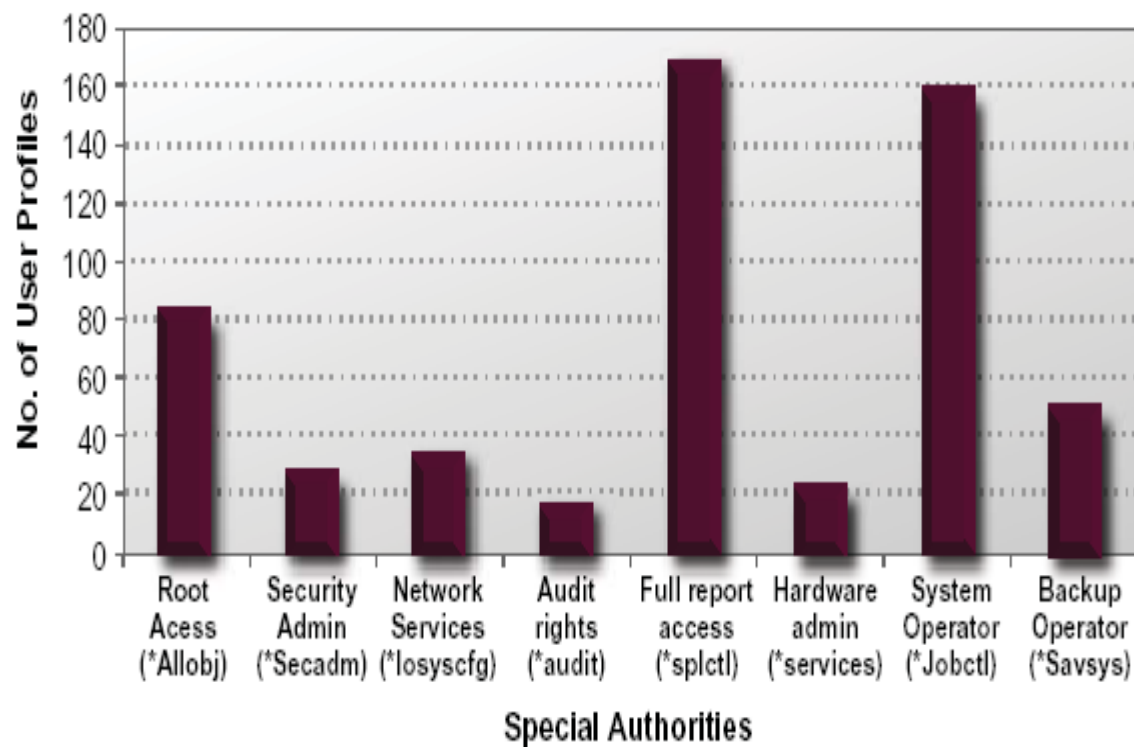


- **Users can be made more powerful through the granting of OS/400 “Special Authorities”**
 - » **Special Authorities can trump OS/400 object level authorities.**
 - A USER WITH ***ALLOBJ** CAN READ, CHANGE, OR **DELETE** ANY OBJECT ON THE SYSTEM.
 - A USER WITH ***SPLCTL** CAN READ, CHANGE, OR **DELETE** ANY SPOOL FILE ON THE SYSTEM.
 - A USER WITH ***JOBCTL** CAN VIEW, CHANGE, OR STOP ANY JOB ON THE SYSTEM (INCLUDES ENDSBS AND PWRDWNSYS)
 - A USER WITH ***SAVSYS** CAN READ OR **DELETE** ANY OBJECT ON THE SYSTEM.

Powerful Users

2

Figure 1 - Powerful Users (Special Authorities)



- **What do special authorities do?**
 - » ***ALLOBJ** - ALL authority to every object on the system – Game Over!
 - » ***AUDIT** - Authority to manipulate system auditing values.
 - » ***IOSYSCFG** - Authority to create and modify communications to the system.
 - » ***JOBCTL** - Authority to control *other* user's jobs.

- **What do special authorities do?**
 - » ***SAVRST** - Authority to save, restore, and remove any object on the system.
 - » ***SECADM** - Authority to change profiles and passwords
 - » ***SERVICE** - Authority to use the system service tools
 - » ***SPLCTL** - ***ALLOBJ** authority for spool files

Learn more at:

<http://www.powertech.com/documents/articles/Exposures.pdf>

Weak or Compromised Passwords

3

- **Passwords can be sniffed in network traffic**
- **Several protocols submit user ID's and passwords in clear text**
 - » **FTP, Telnet, and older forms of Client Access and PC support**
- **Protect yourself by...**
 - » **Minimizing use of legacy OS/400 sign-on screen**
 - » **Set the Client Access "Bypass Signon" Use VPN's when communicating over un-secure networks**

Weak or Compromised Passwords

3

- **Too many passwords, too many places**
 - » Users pick passwords that are easy to remember
 - » Users will re-use passwords inside and outside the company.
 - » Every occurrence of a password is a potential point of exposure.
- **Use Single Sign-On to reduce the number of passwords in your organization**
 - » Don't send passwords via email, or over un-secured networks.
 - » Require that passwords be changed at regular intervals.
 - » Don't use default passwords

Weak or Compromised Passwords



- **If you must have passwords, prevent trivial passwords:**

» At a minimum, set these system values:

<u>System Value Name</u>	<u>Value</u>	<u>Description</u>
• QPWDEXPITV	90	90 Days
• QPWDMINLEN	6	6 Character Minimum length
• QPWDRQDDGT	1	Require a digit
• QPWDRQDDIF	5	Unique in 10

- **Use a password checker to prevent trivial passwords**
- **Use OS/400's Single Sign-On – PowerTech can help!**

Weak or Compromised Passwords



> Why Single Sign-On (SSO)?

- » Password resets are expensive
- » Too many passwords risks disclosure
- » Password synchronization schemes extend the problem
- » IBM and Microsoft provide native support for SSO
- » Password elimination is the most secure approach

User Identity Theft



- **3 ways to steal an OS/400 user ID**
 - **OS/400 Job Description**
 - **Submit Job Command (SBMJOB)**
 - **IBM API's to Switch to the user**
- > **None of these methods requires you to know the user's password**

User Identity Theft



- > **Use an OS/400 job description to masquerade as the user.**
 - » **A JOBID that has a User ID attached to it represents the ability to run a job as that user....**
 - No password required
 - » **Only at QSECURITY level 30 and lower.**
 - » **SBMJOB CMD(CALL MYPGM)
JOB(REPORT) JOBID(QGPL/QBATCH) USER(*JOBID)**
 - » **Solution?**
 - Move to QSECURITY level 40 or higher.

User Identity Theft



- **Use the Submit Job Command (SBMJOB) to masquerade as the user**
- **Specify the name of another user, and run using the assumed identity**
 - SBMJOB CMD(CALL MYPGM)
 - JOB(REPORT) JOBD(QGPL/QBATCH) USER(**SALLY**)

User Identity Theft



- **Use IBM API's to switch to the user**
 - No password required
- **The following code will allow me to become someone else without knowing their password**

- Program QSYS/QASSUME

```
PGM PARM(&USER)
```

```
  DCL      &USER 0
```

```
  DCL      &P 4
```

```
  DCL      &R 0
```

```
  DCL      &S 0
```

```
  DCL      &T 0
```

```
  DCL      &U 0
```

```
  DCL      &V 0
```

```
  DCL      &W 0
```

```
  DCL      &X 0
```

```
END
```



The Open Door Policy

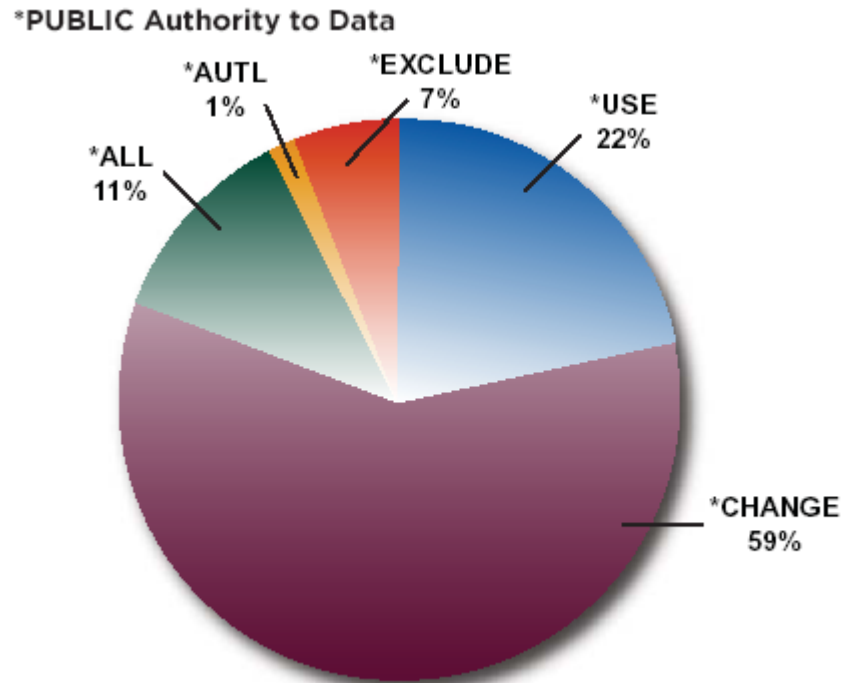
5

- **Every OS/400 object specifies some kind of authority for a user called *PUBLIC?**
 - » **WHO IS *PUBLIC?**
 - Any user of this computer who does not have explicit authority to a given object.
 - » **In the old days *PUBLIC was “Everyone in my company”**
 - Then as we networked to more and more systems, *PUBLIC became every one you do business with (Customers, Vendors, Partners, etc.)
 - With virtually every network connected to every other network (it’s called “The Internet!”), *PUBLIC could be anyone in the WORLD that can connect to your network!!!
 - » **In a perfect world, *PUBLIC should have little or no authority to production applications.**

The Open Door Policy

5

*PUBLIC AUTHORITY TO LIBRARIES



iSeries Security Study 2007

Source: The PowerTech Group Inc.

The Open Door Policy



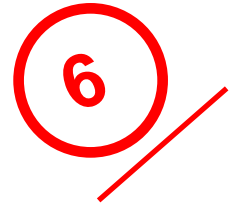
- **At a maximum, Business Application users need no more than;**
 - » *USE authority to static objects such as programs.
 - » *CHANGE Authority to dynamic objects such as data files.
- **Ideally, don't give *PUBLIC even read (*USE) authority to anything**
- **Check out the QCRTAUT system value to see what authority *PUBLIC is given by default to newly created objects.**

Promiscuous Object Ownership



- **All end users belong to a group profile that owns all of the application objects.**
 - » **Easy to administer security**
- **Assumes that all application access will take place through a predefined menu interface**

Promiscuous Object Ownership



- **Why is this a problem?**
 - » **Users are no longer locked into green screen interfaces and dumb terminals.**
 - » **There are numerous ways of getting at the data**
 - Command Line access
 - DFU, DBU, EZView and other Data manipulation tools
 - QUERY/400, SQL, and other query tools
 - FTP, ODBC, Remote command and other network accesses.
 - » **Make sure that you've got all the back doors (and Windows!) covered as well.**

Libraries and Library Lists

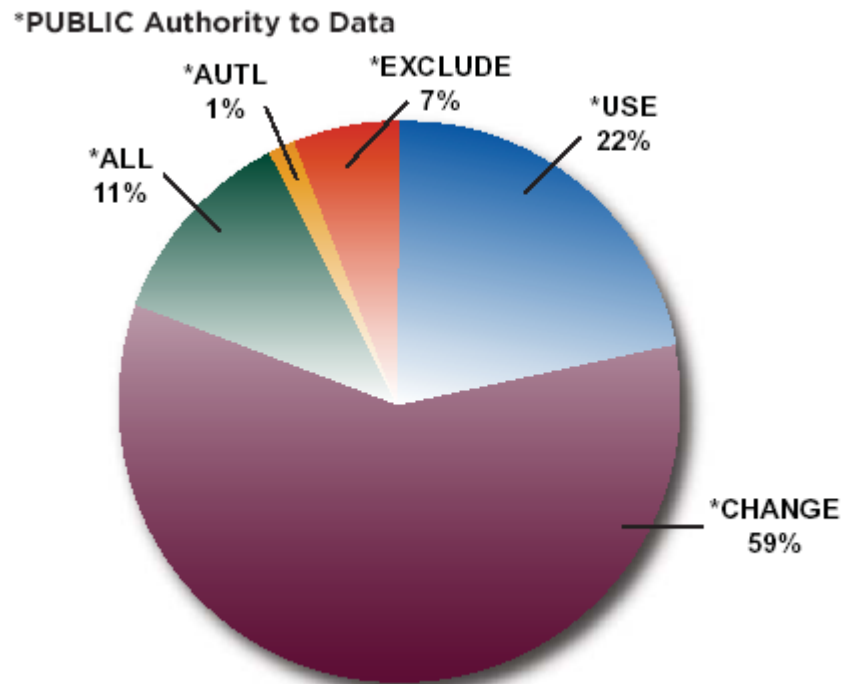


- **A library list specifies the order in which objects and files are searched for.**
- **A user who can place objects into a library could bypass security checking programs**
 - » **Example:**
 - If the library list contains LIBa, LIBb, and LIBc
 - And security checking program PROGZ exists in LIBC
 - And user Fred has at least *USE + *ADD authority to LIBA
 - User Fred could place a bogus version of PROGZ into LIBA that bypasses security
- **Solution:**
 - » **Users only need *USE authority to libraries in their library list.**
 - » **This is especially true of libraries on the system portion of the library list (System Value QSYSLIBL)**

Libraries and Library Lists



*PUBLIC AUTHORITY TO LIBRARIES



iSeries Security Study 2007

Source: The PowerTech Group Inc.

Libraries and Library Lists



- **Protect libraries first**
 - » No more than ***USE** authority to production libraries
 - » ***EXCLUDE** for sensitive libraries
- **User authorities to libraries:**
 - » ***EXCLUDE** => Cannot access anything
 - » ***USE** => Read, change, or **delete** objects
 - » ***USE** plus ***ADD** => Place new objects into a library
 - » ***ALL** => Delete the library

Command Line Abuse

8

- **The ability to execute commands allows a user to skirt traditional menu limitations**
 - » **Commands can be entered in a variety of ways:**
 - OS/400 command line (Call QCMD)
 - OS/400 screens that display a command line (WRKOUTQ, WRKWTR etc.), or other applications with hidden command line access keys.
 - Through the use of the attention key.
 - Using FTP to issue a command remotely
 - Using Client Access to issue a command remotely
 - Using DDM to issue a command remotely

Command Line Interface Abuse



- **Control user's access to commands by...**
 - » **Use the Limited Capability parameter (LMTCPB) on the OS/400 user profile to some interfaces**
 - » **Beware that other interfaces do not respect the LMTCPB parameter limitations**
 - Use an exit program to limit DDM, Client Access, and OPSNAV, and other Windows interfaces
 - » **Some users require command line access (Programmers, Operators, Vendors, etc.)**
 - Make sure that they are monitored

Command Line Interface Abuse

8

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\john.earl>rmtcmd crtlib hacker
IBM iSeries Access for Windows
Version 5 Release 3 Level 0
Submit Remote Command
(C) Copyright IBM Corporation and Others 1984, 2003. All rights reserved.
U.S. Government Users Restricted Rights - Use, duplication or disclosure
restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM
The remote system name is 10.0.1.179.
CPC2102 - Library HACKER created.
C:\Documents and Settings\john.earl>rmtcmd dltlib hacker
IBM iSeries Access for Windows
Version 5 Release 3 Level 0
Submit Remote Command
(C) Copyright IBM Corporation and Others 1984, 2003. All rights reserved.
U.S. Government Users Restricted Rights - Use, duplication or disclosure
restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM
The remote system name is 10.0.1.179.
CPC2194 - Library HACKER deleted.
C:\Documents and Settings\john.earl>
```

System Value Weaknesses



- **There are several system values must be set properly to protect your system**
 - » **Set the system values to their most protective setting**
 - Then toggle them off/on as needed.
 - » **Monitor system values to detect and alert you whenever they are changed.**
 - Ensure that those system values are changed back
 - Monitor for toggle off / toggle on conditions
 - Monitor while System Values are toggled off

System Value Weaknesses



- **Sign-On Control- regulate sign on to prevent attacks**
 - » **QDSPSGNINF = 1**
 - Display the signon information screen.
 - » **QINACTITV = 30**
 - Time out a screen after 30 idle minutes.
 - » **QINACTMSGQ = *DSCJOB**
 - When job is timed out, disconnect job and show signon screen.
 - » **QMAXSIGN = 3**
 - Maximum invalid signon attempts allowed.
 - » **QMAXSGNACN = 2**
 - **Disable User after 'N' invalid signon attempts**
 - » **QRMTSIGN = *VERIFY**
 - Allow user to bypass legacy signon screen.

System Value Weaknesses

9

> **Malicious programs –**
Prevent malicious programs from being loaded to your system by setting these system values:

» **QALWOBJRST = *NONE**

■ Do not allow sensitive program restore.

» **QFRCCVNRST = 1**

■ Force object conversion on restore.

» **QVFYOBJRST = 3**

■ Signed objects must be valid upon restore.

System Value Weaknesses



> Operating system integrity

» QSECURITY

☹️ 10 = Physical Security

☹️ 20 = Password Security

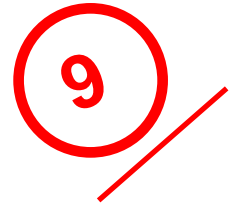
☹️ 30 = Resource Security

✓ 40 = Operating System Security

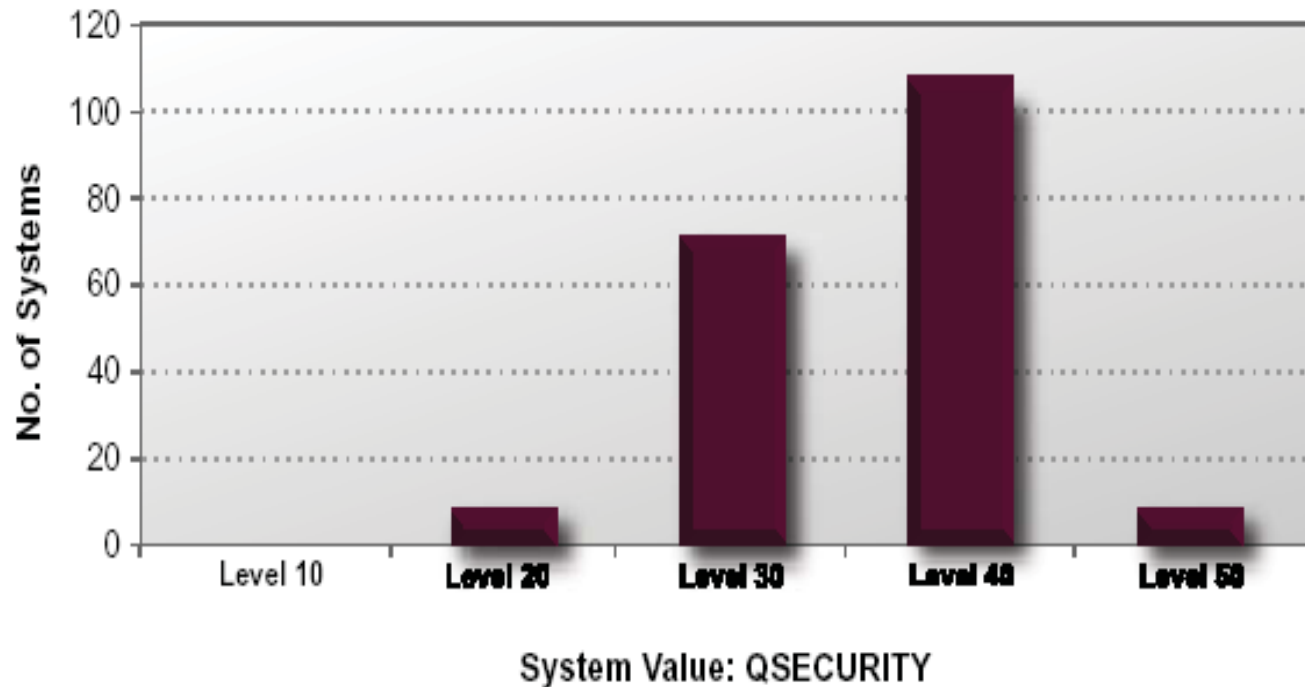
✓ 50 = Enhanced Operating System Security

» **Do not allow programs to bypass OS security**

System Value Weaknesses

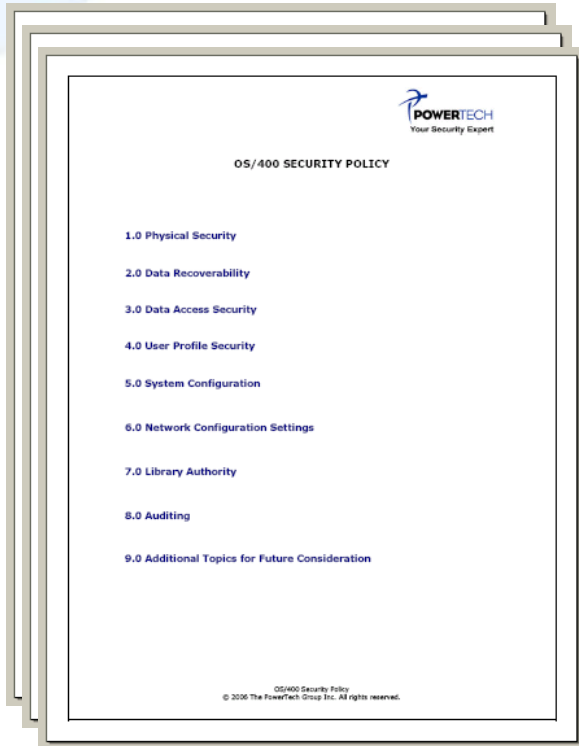


Operating System Integrity - QSECURITY



iSeries Security Study 2007 Source: The PowerTech Group Inc.

PowerTech's Open Source Security Policy



- Free for all attendees!

www.powertech.com/securitypolicy.html

- What does “Open Source” mean?

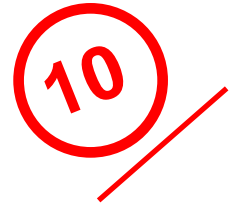
- **If you had a security problem, would you know?**
 - » Who did it?
 - » What happened?
 - » When it happened?
 - » How it was done?
 - » How to stop it from happening again?
- **What if the data was not damaged, but only stolen?**

No Audit Ability



- **In order to prevent security breaches, you must first be able to detect them**
- **Use the OS/400 security auditing journal (QAUDJRN) to help determine where your security stands**
 - » **Why?**
 - It's free (from IBM)
 - It's a comprehensive gathering tool
 - It's an irrefutable source of historical events.

No Audit Ability



- Turn on OS/400 security auditing by typing:

```
CHGSECAUD          QAUDCTL(*AUDLVL)          +
                   QAUDLVL(*AUTFAIL *CREATE *DELETE +
                       *JOBDTA *NETCMN *OBJMGT +
                       *OFCSRV *OPTICAL *PGMADP +
                       *PGMFAIL *PRTDTA *SAVRST +
                       *SECURITY *SERVICE *SPLFDTA +
                       *SYSMGT )          +
                   INLJRNRCV(SECURLIB/AUDRCV0001)
```

- This will generate a lot of audit trails
- Use *tools* to sift through the audit trails to find important events.
- If at all possible, save *all* security journal receivers.
- Make sure QAUDENDACN is *NOTIFY.

Monitoring Compliance on System i

The screenshot displays a software interface with two main windows. The left window, titled 'Security Related System Values', contains a table with the following data:

System Name	System Value	Category
Robinson	QPWDLDPGM	Password
Robinson	QRETSVRSEC	Security
Robinson	QRMTIPL	Restart
Robinson	QRMTSIGN	Restart
Robinson	QRMTSRVATR	Messages and ser
Robinson	QSCANFS	Security
Robinson	QSCANFSCTL	Security
Robinson	QSECURITY	Security
Robinson	QSFWERRLOG	Messages and ser
Robinson	QSHRMEMCTL	Security
Robinson	QSTRUPPGM	Restart
Robinson	QSVRAUTITV	System and user c
Robinson	QSYSLIBL	Library lists
Robinson	QUSEADPAUT	Security
Robinson	QVFOBJRST	Save and Restore
Robinson	ZALWDCRTAD	Security
Robinson	ZALWSTIDCG	Security
Robinson	ZALWSYVLCG	Security
Robinson	ZDDMACCPGM	System and user c
Robinson	ZJOBACN	System and user c
Robinson	ZPCSACCPGM	System and user c
Robinson	ZSECRTYPND	Security
Robinson	ZSYSNAME	System and user c
Tatoosh	QACGLVL	Auditing
Tatoosh	QALWOBJRST	Save and Restore
Tatoosh	QALWUSRDMN	Security
Tatoosh	QATNPGM	System and user c
Tatoosh	QAUDCTL	Auditing
Tatoosh	QAUDENDACN	Auditing
Tatoosh	QAUDFRCLVL	Auditing
Tatoosh	QAUDLVL	Auditing

The right window, titled 'Security System Values', provides a detailed view for the selected 'QSECURITY' value. It includes the following information:

- System Value:** QSECURITY
- PowerTech recommended setting:** 40
- Importance:** Extremely High
- Purpose:** The different security levels and their meanings are listed below:
 - Level 10:** No Security. No password required, and user IDs are created for any user who requests signon. IBM no longer supports level 10.
 - Level 20:** Password Security. Every user must have a valid ID and password. Every user with a valid ID and password assumes root-level authority.
 - Level 30:** Resource Security. Object-level authority is enforced. A moderately knowledgeable programmer or operator can bypass resource-

Compliance Guide

The screenshot displays the PowerTech Compliance Monitor application. The main window title is 'Compliance - Profiles with Default Passwords - /Users/clay/workspace - PowerTech Compliance Monitor'. The interface includes a menu bar (File, Edit, Navigate, Report, Window, Help), a toolbar with 'Contents', 'Index', and 'Search' buttons, and a search field. A left-hand navigation pane lists various compliance categories, with 'Default Passwords' selected and highlighted. The main content area is titled 'Default Passwords' and contains two paragraphs of text. Below the text is a table titled 'Profiles with Default Passwords' showing a list of system profiles.

Default Passwords

Any profile with a password equal to username is an unacceptable security risk. Unfortunately many companies have policies to name their user accounts or profiles based on a standard format, such as first name initial followed by surname (e.g., jsmith, tjones).

These policies enable a hacker to guess profile names like jsmith and try default passwords. It's even easier for an employee who understands internal standards for user profile names to guess account names and to try default passwords.

System Name	Profile	Status	Grp Mbr	Limit Cap	Inv Sgn
Alkipt	APPSEC	*DISABLED	0	*NO	0
Alkipt	ATT2	*DISABLED	0	*NO	0
Alkipt	BINGRP	*DISABLED	0	*NO	2
Alkipt	CAJ3	*DISABLED	0	*NO	0
Alkipt	DKR2	*DISABLED	0	*NO	0
Alkipt	EMGAPPS	*DISABLED	0	*NO	0
Alkipt	HRCHANGE	*DISABLED	0	*NO	0
Alkipt	JTEGRP	*DISABLED	0	*NO	0
Alkipt	LHE	*DISABLED	0	*NO	0
Alkipt	LXG3	*DISABLED	0	*NO	0
Alkipt	RCJ2	*DISABLED	0	*NO	0
Alkipt	TESTPGMR	*DISABLED	0	*NO	0
Alkipt	TESTUSER	*DISABLED	0	*NO	0
Alkipt	TSTGRP	*DISABLED	0	*NO	0
Alkipt	VEN	*DISABLED	0	*NO	2

Best Practices Mapped to COBIT and ISO 17799 Standards

Security System Values

Run the [Security System Values](#) report to determine the current settings for security system values on your system. Compare the system values with the recommended values in chart below. Click on the link in the system value name to learn more about its meaning.

System Value	Description	Audit Importance	PowerTech Recommendation	CobiT	ISO 17799	
QSECURITY	System Security Level	HIGH	40	PO2.4 Security Levels		
QINACTIV	Time-out Period for Inactive Jobs	HIGH	30 = 30 Minutes	CobiT - PO 2.4 Security Levels Management should define, implement and maintain security levels for each of the data classifications identified above the level of "no protection required." These security levels should represent the appropriate (minimum) set of security and control measures for each of the classifications and should be re-evaluated periodically and modified accordingly. Criteria for supporting different levels of security in the extended enterprise should be established to address the needs of evolving e-commerce, mobile computing and telecommuting environments.		
QINACTMSGQ	Action/Message Queue for Inactive Jobs	HIGH	*DSCJOB - or - a monitored message queue name			
QDSCJOBIV	Period before disconnected jobs end	MEDIUM	60 = 60 Minutes			
QDSPSGNINF	Display Sign-on Information	MEDIUM	1 = Display Sign On information			
QMAXSIGN	No of unsuccessful login attempts allowed for this account	HIGH	3			
QMAXSGNACN	Action after number of signon attempts exceeds the max	HIGH	2 = Disable Profile		DS5.2 Identification, Authentication and Access	ISO9.5.2.e
QCRTAUT	Create Default Public	HIGH	*USE, then control at Library Level		DS5.3 Security of Online Access to Data	



Questions?

**Download an open source
Security policy at
www.powertech.com**