IFS Security:
Don’t Leave Your Server Vulnerable

Agenda

- Introductions
- What is the Mysterious IFS and Who Cares?
- IBM i vs. Unix vs. PC
- Batten Down the Hatches!
- Don’t Forget About Viruses
- Resources for Security Officers
- Questions and Answers

Today's Speaker

Robin Tatam

Director of Security Technologies

robin.tatam@powertech.com

Who is PowerTech?

- Premier Provider of Security Solutions & Services
  - 16 years in the security industry as an established thought-leader
  - Customers in over 70 countries, representing every industry
  - Security subject-matter-expert for COMMON
- IBM Advanced Business Partner
- Member of PCI Security Standards Council
- Authorized by NASBA to issue CPE Credits for Security Education
- Publisher of the Annual “State of IBM i Security” Report

NASBA
National Association of State Boards of Accountancy

IBM Business Partner

PCI Security Standards Council™

What Is the Mysterious IFS?

(and who cares?)

What Is the Mysterious IFS?

According to Wikipedia, it can be many things to many people:

- Independent Front Suspension
- Indian Fertility Society
- Initial Flight Screening
- Initiative on Financial Security
- Institute for Fiscal Studies
- Insurance and Financial Services
- Intensive Freshman Seminar
- International Financial Statistics
- International Food Standard
- Integrated Forecast System

What Is the Mysterious IFS?

Integrated File System

Integrated File System - on IBM midrange & mainframe systems (e.g. OS/400, MVS, VM/CMS), the POSIX compatible file system provided by the operating system, as opposed to the traditional non-POSIX file system it also supplies.

What Is the Mysterious IFS?

- Added to OS/400 in V3R1 in 1994
- Integrates IBM i with UNIX, Windows, and others
- Directory structure much like a PC
- Provides access to data stored on integrated servers, or on other remote IBM i servers
- Contains several pre-defined file systems:
  - All contained within a single root directory
  - Each with their own limitations and rules

What Is the Mysterious IFS?

Contrary to popular belief, it was not an add-on to the existing file structures, but rather encompasses ALL of the file structures. This includes those that pre-date the IFS such as:

Native Libraries	**\QSYS.LIB**
Documents and Folders	**\QDLS**

Am I Even Using the IFS?

We ALL technically use the IFS as it encompasses \QSYS.LIB

Some other common uses of the IFS include:

- Integrated PC Servers (Intel processor)
- NetServer (Explorer access to the IFS)
- CD images for unattended installation
- PASE environment for UNIX applications
- IBM i Access (Client Access) & Navigator executables
- Apache HTTP server
- Tomcat Application Server
- WebSphere Application Server
- Lotus Domino
- Digital Certificate Manager

It's Already Secure, Right?

IBM i ships with its public access default set to:

Native objects = *CHANGE

IFS root folder = *RWX
plus all object authorities
(aka *ALL)

TIP: ***This should be changed ASAP!***

“Bill wouldn’t do anything wrong!”

Organizations often place tremendous trust in the people accessing their servers.

Authorized users usually have privileges far in excess of any business requirement.

“Bill wouldn’t do anything wrong!”

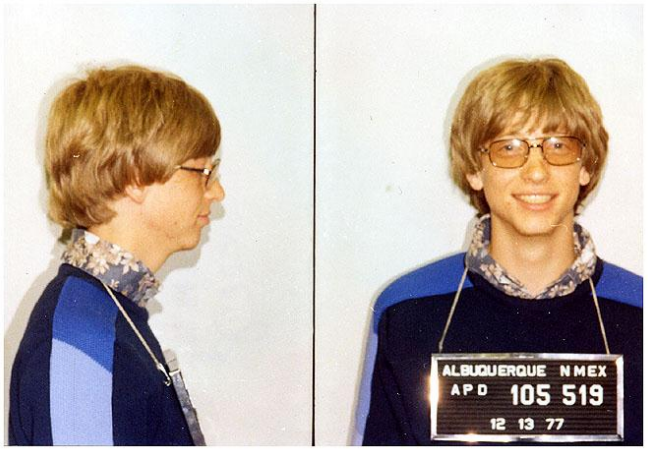
According to the “State of IBM i Security” study, most organizations are still basing security on lack of user knowledge or malicious intent.

- Average of 58 users with *ALLOBJ special authority
- Average of 60 enabled profiles with default passwords

How well do you *really* know Bill?

The reality is that an economic downturn may cause (normally) trustworthy users to act out of desperation.

Of course, anyone can make a legitimate mistake!



IBM i vs. Unix vs. PC

Object Authority vs. Data Authority

In IBM i, every object has data authorities and object authorities.

Data authorities consist of:

Read, Add, Update, Delete, and Execute.

Object Authorities consist of:

Opr, Mgt, Exist, Alter, and Ref.

IBM i authorities (data and object) are typically assigned using IBM-supplied templates:

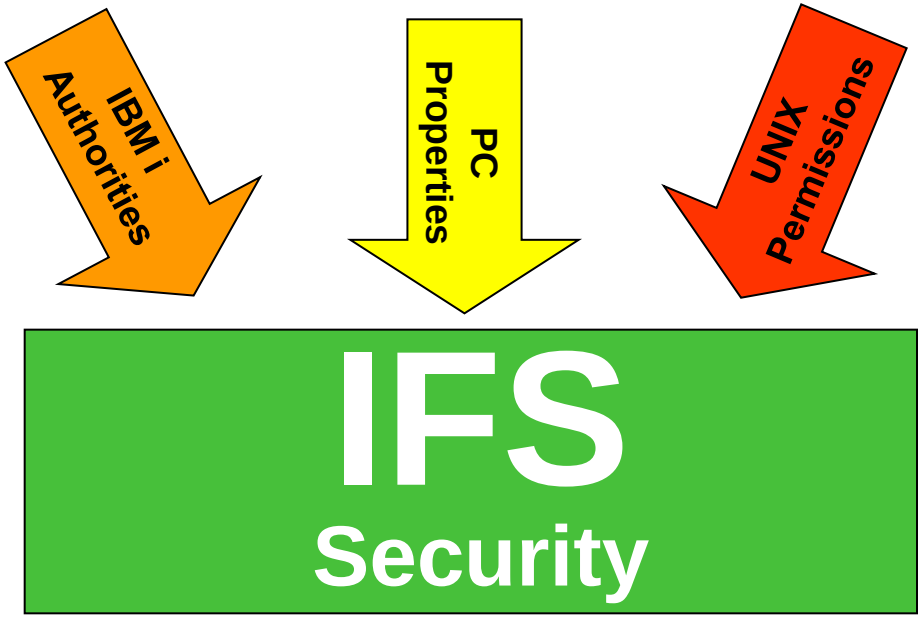
***USE, *CHANGE, *ALL, and *EXCLUDE**

IBM i Authorities

- Data Authorities
  - *READ - Required to read the object
  - *ADD, *UPD, *DLT - Required to change the object
  - *EXECUTE - Required to run a program or find an object
- Object Authorities
  - *OBJOPR - Required to operate on data (set if there are any data authorities)
  - *OBJMGT - Required to move, rename, or work with permissions
  - *OBJEXIST - Required to delete, save, and restore the object
  - *OBJALTER - Database authority
  - *OBJREF - Database authority
- System-Defined “Sets of Authority"
  - *ALL - All data and object authorities
  - *CHANGE - *OBJOPR and all data authorities
  - *USE - *OBJOPR and *READ and *EXECUTE
  - *EXCLUDE - Specifically denies access to the object

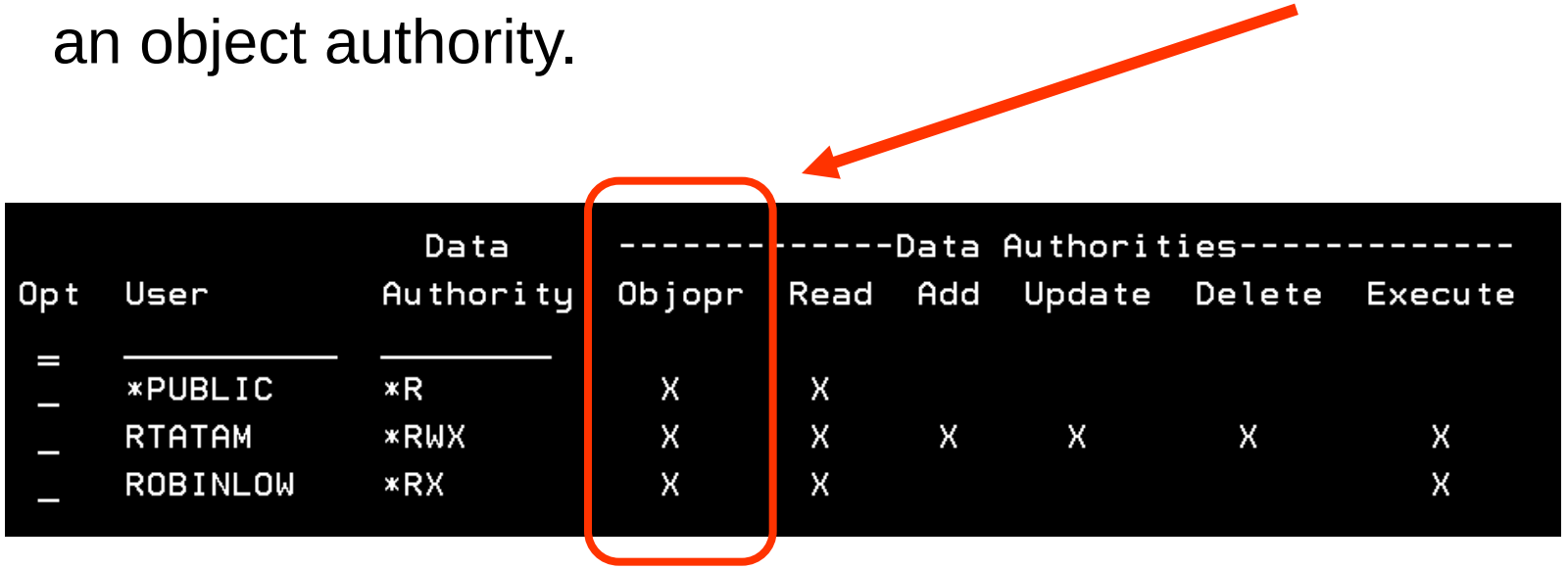
Authorities vs. Permissions

The IFS security model is a unique combination of IBM i authorities, PC file properties, and Unix file permissions.



Object Authority vs. Data Authority

For IFS objects, ‘Opr’ (Object Operational) authority is considered a data authority and NOT an object authority.



Opt	User	Data Authority	Data Authorities: Objopr	Read	Add	Update	Delete	Execute
=								
_	*PUBLIC	*R	X	X				
_	RTATAM	*RWX	X	X	X	X	X	X
_	ROBINLOW	*RX	X	X				X

Unix Permissions

In Unix terminology, we secure files and directories using a combination of Read (*R), Write (*W), and Execute (*X) permissions.

***USE**

As with *USE, *RX provides Read and Execute data authority and no object authorities (except ‘Opr’ as noted on the prior slide)

***CHANGE**

As with *CHANGE, *RWX provides all data authorities and no object authorities (except ‘Opr’ as noted on the prior slide)

There’s no UNIX equivalent of *ALL

PC Properties

PC properties, such as “read-only”, are another layer of protection against misuse. Even *ALLOBJ users cannot delete a file that is marked as read-only.

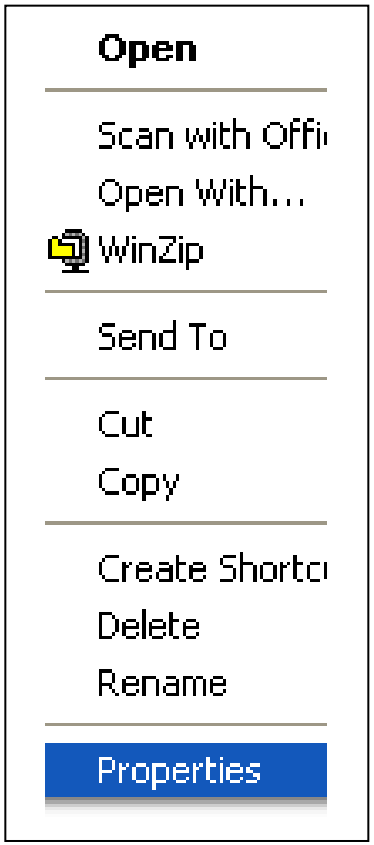
Other file properties include:

- Need to Archive (PC and System)
- Hidden File
- PC system file

PC Properties

PC Properties can be viewed and altered using:

- IBM i's CHGATR command
- Navigator for i properties
- Windows Explorer Properties (NetServer)
- DOS "attrib" commands



PC Properties

IBM i supports a check-out / check-in capability that restricts certain functions to the user that has checked out the file. This process can be performed via:

- Navigator for i
- Check Out (CHKOUT) Command
- Check In (CHKIN) Command

IBM added subtree support in v6.1 so that users can now check out/in entire folders or directories.

IBM i Authorities

Under the covers, all IFS objects are still IBM i objects and therefore have IBM i authorities.

Actions must still meet the requirements set forth by IBM i.

For example:

*To delete a stream file, you must have *OBJEXIST authority. This is an object authority that's not associated with *R, *W, or *X and must be granted separately, or inherited from the directory.*

Batten Down the Hatches!

PowerTech
your security expert

It All Starts at the "Root"

It's easy to "over secure" the IFS due to the nature of nested directories and unfamiliar security mechanisms.

Plan carefully and make detailed notes of changes so that you can always change back if there is a problem.

With the exception of 'root,' most IBM directories are already configured with the appropriate security settings. Vendor directories may not be.

Remove the Right to Write

The “root” (/) folder ships with powerful *PUBLIC permissions:

DTAAUT(*RWX)

OBJAUT(*ALL)

Instead, consider assigning the following:

DTAAUT(*RX)

OBJAUT(*NONE)

Do NOT set *PUBLIC to *EXCLUDE

Remove the Right to Write

A user requires *X authority to each directory in the folder structure. However without *R they cannot see the contents of the directory.

Consider whether a user should be able to access (read or write) the contents of the parent folder(s) or just simply navigate to a subfolder.

Remove the Right to Write

Consider giving users their own directory under "/home"

Set DTAAUT(*X) for *PUBLIC on '/home'

Set DTAAUT(*EXCLUDE) for *PUBLIC on all user directories

Set DTAARA(*RWX) for the user on their own directory (e.g. '/home/rtatam')

This enables a user to access their own directory, but not to touch (or see) other users' directories.

Remove the Right to Write

IFS Permissions can be assigned through a traditional green screen interface, using:

WRKAUT, CHGAUT, DSPAUT

Or, through the (Systems Director) Navigator for i interface.

Restrict Access to QSYS.LIB

Most organizations don't need users to be able to access the native libraries and objects from remote clients like IBM i Access, NetServer, and Java Toolbox.

Fortunately, IBM provides an authorization list to control who can access QSYS.LIB:

Authorization List	QPWFSERVER
Default *PUBLIC	*USE
Recommended *PUBLIC	*EXCLUDE

Warning: Not effective against *ALLOBJ users

Manage File Shares

Many organizations make their IFS accessible to client users by establishing unnecessary file shares. Use IBM i Navigator to:

- Eliminate unnecessary file shares
- Make shares “Read Only” when possible
- Grant only *X permission to folders in shared path
- Do NOT share the ‘root’ (/) folder

Don’t give all users access to IBM i Nav

Audit IFS Object Access

Similar to auditing of IBM i objects, the IFS also supports event auditing.

- Ensure QAUDCTL system value includes the value of *OBJAUD to “turn on” object auditing
- Use CHGAUD command to specify the desired level of auditing for each object or directory

Also deploy exit programs to help audit events

Audit IFS Object Access

As with libraries, each directory has a Create Object Auditing (CRTOBJAUD) value to designate the auditing of the contents.

You need audit (*AUDIT) or all object (*ALLOBJ) special authority to see the auditing setting:

***SYSVAL, *USRPRF, *CHANGE, *ALL, *NONE**

Secure Native Commands

IFS commands are (by default) secured from limited capability users - LMTCPB(*YES).

Command-capable users might have access to the following powerful native IFS commands:

Command(s)	Shipped *PUBLIC
WRKLNK	*USE
MD | MKDIR | CRTDIR	*USE
RD | RMDIR | RMVDIR	*USE
CD | CHGDIR | CHGCURDIR	*USE

Secure Native Commands

Other powerful IFS commands to be guarded include:

CPYTOSTMF	Copy to Stream File
CPYFRMSTMF	Copy From Stream File
CPYTOIMPF	Copy To Import File
CPYFRMIMPF	Copy From Import File
WRKAUT | CHGAUT	Work | Change Authority
CHGOWN	Change Owner
SAV | RST	Save | Restore

Authority Adoption & Profile Switching

The IFS does NOT support the adoption of authority. This can represent a challenge to applications that are built on a foundation of adoption.

Profile switching is supported, so use the IBM-provided APIs or use a tool like Authority Broker to temporarily alter user privileges—akin to Superman's phone booth.

IFS Is At the Mercy of Other Controls

Another Reason for an Exit Program!

Exit Points enable a process to be temporarily “interrupted” by a user-written program.

There’s an exit point for FTP and ODBC, and yes, IFS!

(Strongly) Consider implementing an exit program to audit and control actions affecting the IFS.

Another Reason for an Exit Program!

The IFS exit point provides easy-to-interpret interrogation and supplemental control of user activities, including:

- Allocate conversation
- Change file attributes request
- Create stream file or directory
- Delete file or directory
- List file attributes (or directory contents)
- Move file
- Open stream file
- Rename file

Works with *ALLOBJ users

Another Reason for an Exit Program!

An example of recording user activities within the IFS using an exit program:

```
Run Date:  5/22/12                        PowerTech Network Security                        Page      :     2
Run Time: 13:50:09              Selected Server All Functions - Rejected Transactions       Run on system: ROBINSON
Run By  : PAULC                          For System ROBINSON, partition   0                Program Name : LNSR087B
Action IP Address or   Server     Function      Transaction    Active
Taken  Location        Name       Name         Date     Time   User       Job Number/User/Name
------ --------------- ---------- ---------- -------- -------- ---------- --------------------------
Reject 192.168.024.034 *FILESRV   LSTSTRMATR 05/22/12 13:47:45 PAULC     283896/QUSER/QPWFSERVSO
     Transaction Data: /home/Payroll
Reject 192.168.024.034 *FILESRV   LSTSTRMATR 05/22/12 13:47:46 PAULC     283896/QUSER/QPWFSERVSO
                                                                                          More...
F3=Exit   F12=Cancel   F19=Left   F20=Right   F24=More keys
```

Don’t Forget About Viruses!

On IBM i? Surely Not!

Long thought to be immune to the virus threat, the IBM i can actually act as the **source** of virus problems on your network.

While malicious code can reside natively, viruses most often impact the IFS.

How Viruses Can Spread Via IBM i

Mapped Drives

FTP

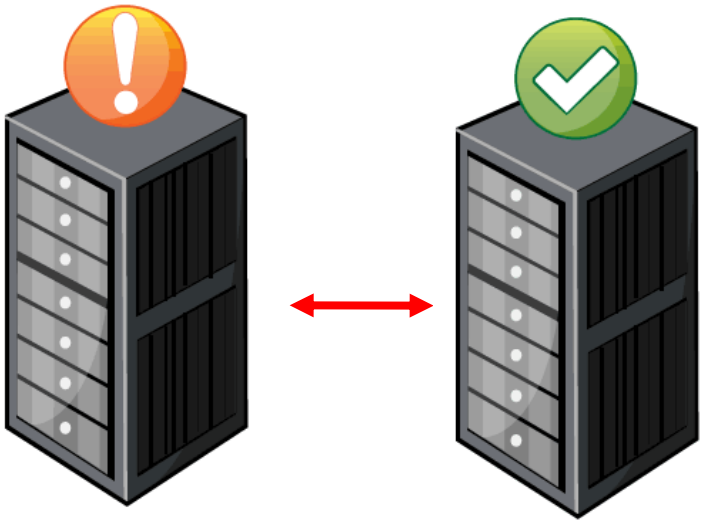
Image Catalogs,
NSF Mounts, UDFS Mounts

Business Partners

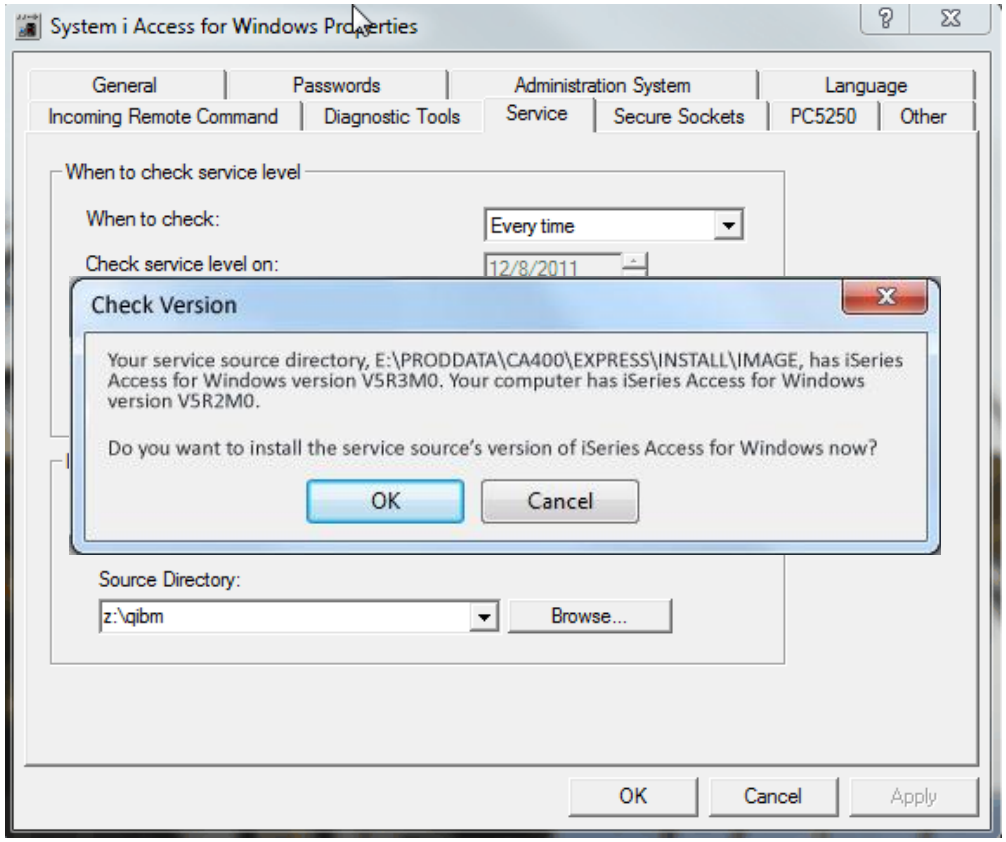
CDs

High Availability Systems

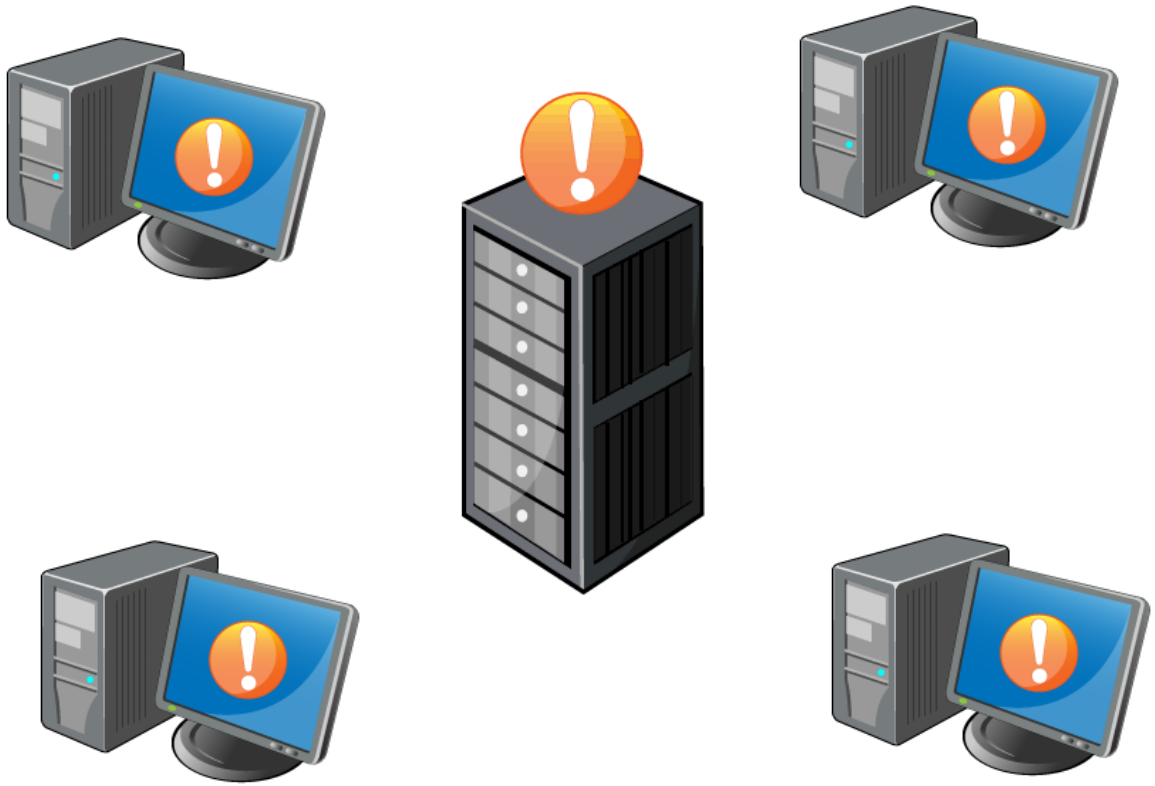
Backup Tapes



How Viruses Can Spread Via IBM i



How Viruses Can Spread Via IBM i



Immunize IBM i with Virus Protection

IBM i added system values (QSCANFS, QSCANFSCTL) to interface with a commercial scanning solution for:

- On-demand Scanning
- Open/Close Scanning (V5R3+) via Exit Point integration

  QIBM_QP0L_SCAN_OPEN – IFS Scan on Open
  QIBM_QP0L_SCAN_CLOSE – IFS Scan on Close
- Object Integrity
- Alerting

Check out StandGuard Anti-Virus From Bytware

PowerTech
your security expert

Don’t Scan From The Network …

Scanning from another server is BAD for several compelling reasons:

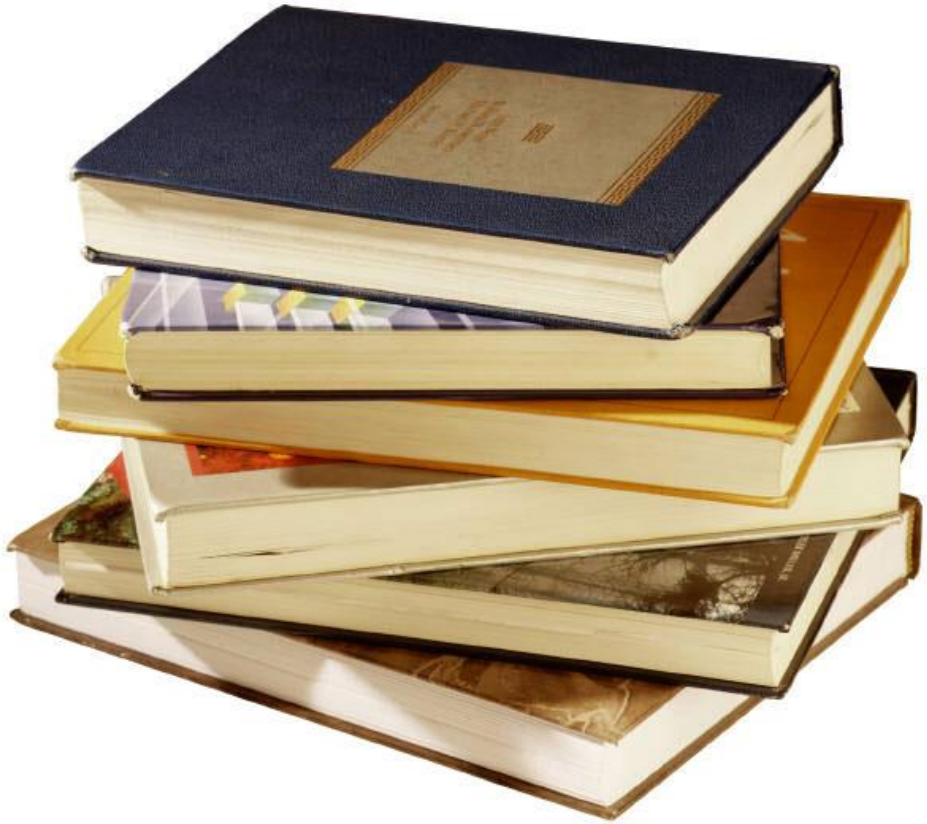
- Requires a read/write share to “root” to search and cleanse all directories
- Requires an *ALLOBJ profile to effectively run the scan
- Network bandwidth is consumed by hundreds of thousands of objects being moved around
- Transmits all objects in clear text

Or You Might Make A Bad Situation Even Worse!

In Summary

- Determine what applications are using the IFS
- Understand how security works on the IFS
- Establish security for top-level folders like “root” and “/home”
- Secure access to /QSYS.LIB
- Monitor and protect file shares (don’t share “root”) and make them read-only whenever possible
- Audit and alert on user activities using an exit program
- Protect from viruses
- *Test your security!*

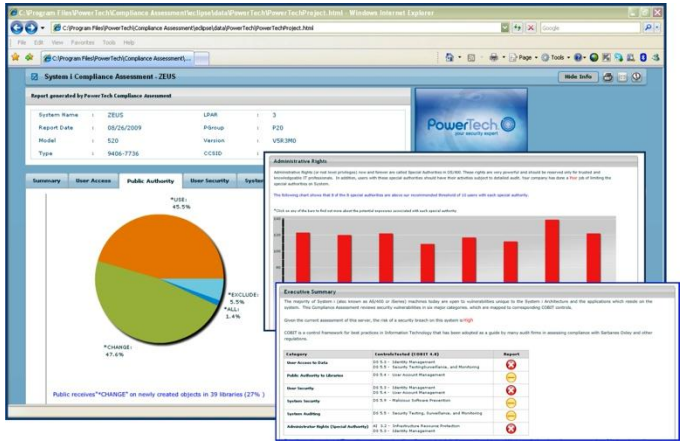
Resources for Security Officers



PowerTech Compliance Assessment

Your PC

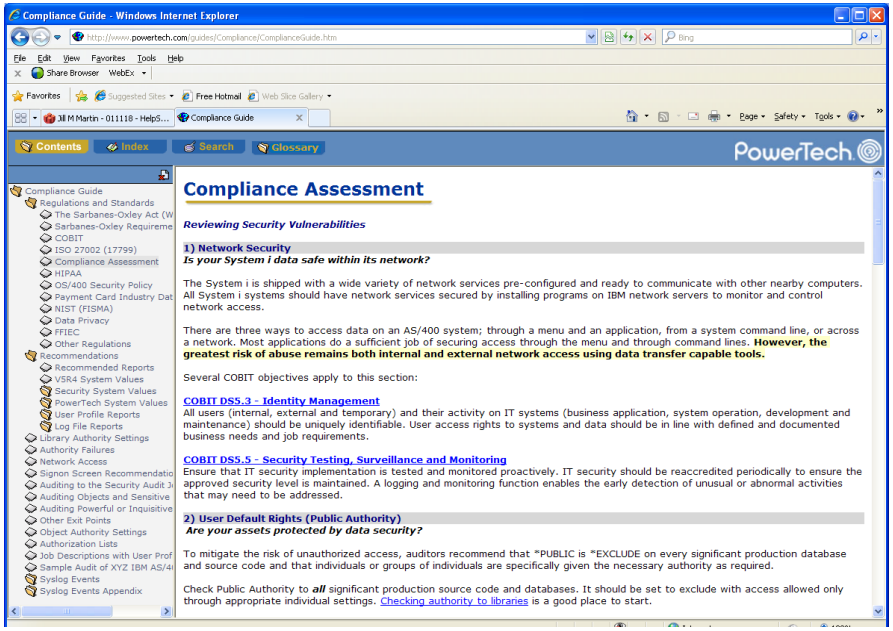
Your Power Systems server



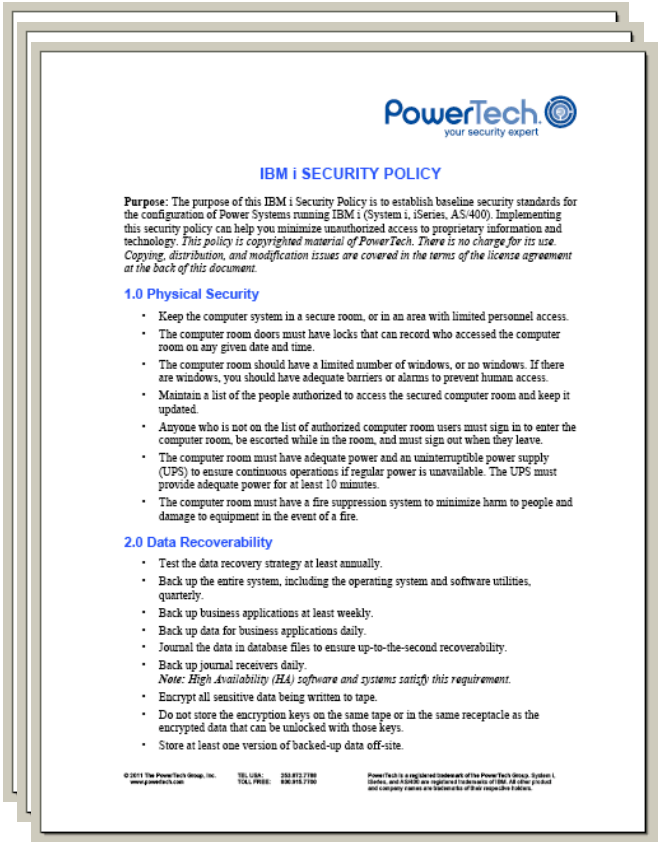
Your Vulnerabilities

Compliance Resources

Online Compliance Guide



Security Policy


PowerTech
your security expert

IBM i SECURITY POLICY

Purpose: The purpose of this IBM i Security Policy is to establish baseline security standards for the configuration of Power Systems running IBM i (System i, iSeries, AS/400). Implementing this security policy can help you minimize unauthorized access to proprietary information and technology. *This policy is copyrighted material of PowerTech. There is no charge for its use. Copying, distribution, and modification issues are covered in the terms of the license agreement at the back of this document.*

1.0 Physical Security

- Keep the computer system in a secure room, or in an area with limited personnel access.
- The computer room doors must have locks that can record who accessed the computer room on any given date and time.
- The computer room should have a limited number of windows, or no windows. If there are windows, you should have adequate barriers or alarms to prevent human access.
- Maintain a list of the people authorized to access the secured computer room and keep it updated.
- Anyone who is not on the list of authorized computer room users must sign in to enter the computer room, be escorted while in the room, and must sign out when they leave.
- The computer room must have adequate power and an uninterruptible power supply (UPS) to ensure continuous operations if regular power is unavailable. The UPS must provide adequate power for at least 10 minutes.
- The computer room must have a fire suppression system to minimize harm to people and damage to equipment in the event of a fire.

2.0 Data Recoverability

- Test the data recovery strategy at least annually.
- Back up the entire system, including the operating system and software utilities, quarterly.
- Back up business applications at least weekly.
- Back up data for business applications daily.
- Journal the data in database files to ensure up-to-the-second recoverability.
- Back up journal receivers daily.
  Note: High Availability (HA) software and systems satisfy this requirement.
- Encrypt all sensitive data being written to tape.
- Do not store the encryption keys on the same tape or in the same receptacle as the encrypted data that can be unlocked with those keys.
- Store at least one version of backed-up data off-site.

PowerTech
your security expert

Other (FREE) Resources

- The State of IBM i Security Study
- Online Compliance Guide
- Webinars / Education Events
- Articles and White Papers
- Security Blog (www.powertechblog.com)
- Twitter (www.twitter.com/powertechgroup)
- PowerNews (www.powertech-news.com)

Find all this at www.powertech.com

Questions

THANK YOU.

Contact Information:

www.powertech.com

(253) 872-7788

sales@powertech.com