www.SecureMyi.com

CyberWar 2015 – Protecting IBM i

Common Security Misconceptions and Vulnerabilities on IBM i

SecureMyi Security Newsletter
The Independent Source for Security for IBM i (ISeries and AS/400)

Presented by Dan Riehl

Dan.Riehl@SecureMyi.com

www.SecureMyi.com

Common Misconceptions

- **The First Step – User Passwords – An Easy Entry Point?**
  - Default Passwords, Harvesting Passwords, Sharing Passwords
- **Special Service Profiles – Initial Program and Menu**
- **User Limited Capabilities (i.e. LMTCPB(*YES))**
- **The User Class - *SECOFR, *SECADM, *SYSOPR *PGMR *USER…**
- **Misconceptions about Ownership and Authority to User Profiles**
- **Misconceptions about Object Authority when using Authorization Lists**
- **Is your system vulnerable to a Virus, Worm or other malware?**

www.SecureMyi.com

2

Initial Password on CRTUSRPRF

The Default Password value is the User name

- Causes exposure for these profiles

```
                    Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . . . . . .   BSMITH      Name
User password  . . . . . . . . .   *USRPRF     Character value, *USRPRF...
Set password to expired  . . . .   *NO         *NO, *YES
Status . . . . . . . . . . . . .   *ENABLED    *ENABLED, *DISABLED
User class . . . . . . . . . . .   *USER       *USER, *SYSOPR, *PGMR...
Assistance level . . . . . . . .   *SYSVAL     *SYSVAL, *BASIC, *INTERMED...
Current library  . . . . . . . .   *CRTDFT     Name, *CRTDFT
Initial program to call  . . . .   *NONE       Name, *NONE
  Library  . . . . . . . . . . .               Name, *LIBL, *CURLIB
Initial menu . . . . . . . . . .   MAIN        Name, *SIGNOFF
  Library  . . . . . . . . . . .     *LIBL     Name, *LIBL, *CURLIB
Limit capabilities . . . . . . .   *NO         *NO, *PARTIAL, *YES
Text 'description' . . . . . . .   *BLANK
```

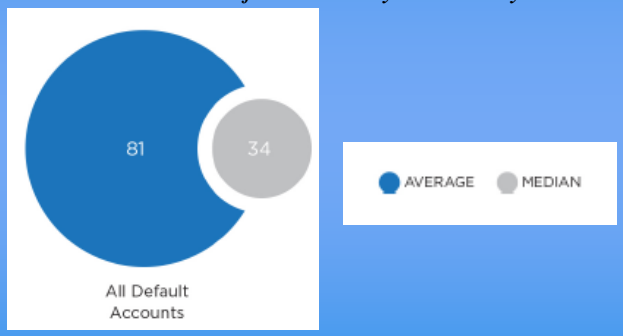
But, we set it to Expired! So It's OK..?

3

Default Passwords - How many do you have?

Nearly 5 percent of enabled user profiles have default passwords. More than half (53 percent) of the systems in the study have more than 30 user profiles—15 percent have more than 100 user profiles—with default passwords.

Source: PowerTech - The State of IBM i Security 2014 – 233 Systems



Check your System - ANZDFTPWD command

4

Simple Harvesting of Passwords

STRCMNTRC CFGOBJ(LINETH) +
CFGTYPE(*LIN) MAXSTG(256K) TEXT('My test trace')

```
                                   Display Spooled File
File  . . . . . :   QPCSMPRT                                                    Page/Line   16/40
Control . . . . .   -5                                                           Columns     1 - 130
Find  . . . . . .   ____________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
                    0000000000000000 000000000000                                *...............
   114   R       46  20:31:51.640890            FFFFFFFFFFFF  30E4DB1F40E4   ETHV2   Type: 0806
       Data . . . . . :  0001080006040001 30E4DB1F40E4C19E  1541000000000000 C19E154300000000   *.........U.. UA.........A......
                    0000000000000000 000000000000                                *...............
   115   R       77  20:31:51.816157            00145E541CA2  D4CA6D4479A2   ETHV2   Type: 0800
       Data . . . . . :  4500004D62C04000 6B06218418D8BC77  B2F9031EC43D0017 AA59E5AFFA14B2DE   *...(.{ ,...D.Q...9..D......V....
                    501840B9EB3D0000 002312A000000400  00030835F1110635 C4C1D5D7E6C41107   *&. ..................1...DANPWD.
                    35D4E8D7C1E2E2E6 D6D9C4FFEF                                  *.MYPASSWORD..
 COMMUNICATIONS TRACE       Title: My test trace                    01/07/15  20:32:12                          Page:      17
 Record       Data    Record           Controller  Destination   Source        Frame            Number  Number    Poll/
 Number  S/R  Length  Timer            Name        MAC Address   MAC Address   Format  Command  Sent    Received  Final  DSAP  SSA
 ------  ---  ------  ---------------  ----------  ------------  ------------  ------  -------  ------  --------  -----  ----  ---
   116   S       40  20:31:52.020532              D4CA6D4479A2  00145E541CA2   ETHV2   Type: 0800
```

***SERVICE Special Authority Needed**
Or WRKFCNUSG customization – or Sniffer
Use encrypted sessions to avoid this

www.SecureMyi.com

5

Sharing Passwords!
What is her Password?
and QSECOFR?

www.SecureMyi.com

6

Shared Passwords

- **One user Profile and Password shared by multiple users**
  - Violates audit and control standards
  - No accountability for actions to the individual user
  - Seen often on Manufacturing Shop Floor, Retail Desk, Casino Floor
  - If you have this audit control defect, make sure your security policy and IT auditors support it, along with your **compensating controls**
- **Used for QSYSOPR, QSECOFR, XXXUSER**
- **Often seen in a common NetServer Log-On for Mapped Drive**
- **Often used for the Sign-on Server Log-On**
  - Very dangerous!
  - Typically means all ODBC, file transfers, all IBM i Access functions run under the shared ID
- **No Sharing of Passwords!**

Common Misconceptions

Special Service Profiles

Initial Program and Menu

www.SecureMyi.com

Initial Pgm *NONE – Menu *SIGNOFF

```
                    Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . . . . . . > DANSIGNOFF    Name
User password  . . . . . . . . .   w2h8e7cc6     Character value, *USRPRF...
Set password to expired  . . . .   *NO           *NO, *YES
Status . . . . . . . . . . . . .   *ENABLED      *ENABLED, *DISABLED
User class . . . . . . . . . . .   *USER         *USER, *SYSOPR, *PGMR...
Assistance level . . . . . . . .   *SYSVAL       *SYSVAL, *BASIC, *INTERMED...
Current library  . . . . . . . .   *CRTDFT       Name, *CRTDFT
Initial program to call  . . . .   *NONE         Name, *NONE
  Library  . . . . . . . . . . .     __________   Name, *LIBL, *CURLIB
Initial menu . . . . . . . . . . > *SIGNOFF      Name, *SIGNOFF
  Library  . . . . . . . . . . .     *LIBL        Name, *LIBL, *CURLIB
Limit capabilities . . . . . . .   *NO           *NO, *PARTIAL, *YES
Text 'description' . . . . . . .   *BLANK
```

Misconception
If Initial Program = *NONE and Menu = *SIGNOFF, means the user Cannot Sign On

www.SecureMyi.com

9

Initial Menus/Programs

- **Reality**
  - **These values apply only to Workstation logon settings.**
    - Can still be used for FTP, REXEC, ODBC, Signon Server, RMTCMD, etc
- **Circumventions**
  - **1) The user *may* be able to specify alternate initial menus and programs from the sign-on screen.**
  - **2) Press Attn Key – to get access**
  - **3) Press SysRqs to get access**
  - **4) The CHGPRF command can be used by a user to change their initial Menu/Program**

10

1) The user *may* be able to specify alternate initial menus and programs from the sign-on screen.

```
                                Sign On
                                          System  . . . . . :   SECURMYI
                                          Subsystem . . . . :   QINTER
                                          Display . . . . . :   DANB1

   User  . . . . . . . . . . . . . .   DANPWD____
   Password  . . . . . . . . . . . .
   Program/procedure . . . . . . . .   QCMD______
   Menu  . . . . . . . . . . . . . .   MAIN______
   Current library . . . . . . . . .   HRDBFA____
```

Fix this Problem by

1) Removing these fields 3 from the sign-on screen
   - Leave fields but use the Protect and Non-Display Attribute

2) AND, Set the User to Limit Capabilities (*YES)

www.SecureMyi.com

Copyright© 2011-2015 Dan Riehl

11

2) Press Attn Key – to get access

```
                        Display Program Messages

Job 460244/DANSIGNOFF/DANB1 started on 01/07/15 at 21:31:36 in subsystem QIN
Initial program ended and *SIGNOFF specified for initial menu.



Press Enter to continue.
```

No Law that you must Press Enter!
Simply Press the Attn Key to get Attn Program

- **The Default is the ASSIST MENU**

Fix by setting User's Attn Program to *NONE

www.SecureMyi.com

Copyright© 2011-2015 Dan Riehl

12

3) Press SysRqs to get access

```
                                   System Request

Select one of the following:

     1. Display sign on for secondary job
     2. End previous request
     3. Display current job
     4. Display messages
     5. Send a message
     6. Display system operator messages
     7. Display work station user

    80. Disconnect job

    90. Sign off



Selection
     3_
```

Can view job Info including Library List and list objects in libraries

The SYSRQS key can be used to acquire a full list of your application libraries and database files, along with the description of each database file, e.g. PAY001P - Payroll Master File.

And, in a little known hacking exploit, the SYSRQS key can be easily be used to enumerate all of the users enrolled on the system.

www.SecureMyi.com

13

Enumerating Users in QUSRSYS

```
                                   Display Library

Library  . . . . . . . :   QUSRSYS         Number of objects  . :   1640
Type . . . . . . . . . :   PROD            Library ASP number . :   1
Create authority . . . :   *SYSVAL         Library ASP device . :   *SYSBAS
                                           Library ASP group  . :   *SYSBAS

Type options, press Enter.
  5=Display full attributes   8=Display service attributes

Opt  Object      Type      Attribute                Size  Text
 _   SCCLLLIMIT  *MSGQ                             12288
 _   SCCLLUSER1  *MSGQ                             12288
 _   SCCLLUSER2  *MSGQ                             12288
 _   SCDER       *MSGQ                             12288  Dans group
 _   SCDERLIMIT  *MSGQ                             12288  Dan R Limited User
 _   SCDERUSER1  *MSGQ                             12288  Dans User 1
 _   SCDERUSER2  *MSGQ                             12288  Dans User 2
 _   SCHERERH    *MSGQ                             12288  RZKH administrative a
 _   SCKUF       *MSGQ                             12288  Kathy's attempt at a
 _   SCKUFLIMIT  *MSGQ                             12288
```

Fix by Restricting Access to SysRQS Key (by Securing The Panel group)

Restrict Access to *PUBLIC

GRTOBJAUT OBJ(QSYS/QGMNSYSR) OBJTYPE(*PNLGRP) USER(*PUBLIC) + AUT(*EXCLUDE)

And Grant Access to your IT Group

GRTOBJAUT OBJ(QSYS/QGMNSYSR) OBJTYPE(*PNLGRP) USER(IT_GROUP) AUT(*USE)

www.SecureMyi.com

14

4) The CHGPRF command can be used by a user to change their own initial Menu/Program

- CHGPRF – Change my User Profile
- Users can change their own User Profile

```
                          Change Profile (CHGPRF)

Type choices, press Enter.

Assistance level . . . . . . . .   *SYSVAL       *SAME, *SYSVAL, *BASIC...
Current library  . . . . . . . .   RPGCLASS8     Name, *SAME, *CRTDFT
Initial program to call  . . . .   *NONE         Name, *SAME, *NONE
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Initial menu . . . . . . . . . .   MAIN          Name, *SAME, *SIGNOFF
  Library  . . . . . . . . . . .     *LIBL       Name, *LIBL, *CURLIB
Text 'description' . . . . . . .   'Dan Riehl'

                        Additional Parameters

Keyboard buffering . . . . . . .   *SYSVAL       *SAME, *SYSVAL, *NO...
Job description  . . . . . . . .   QDFTJOBD      Name, *SAME
  Library  . . . . . . . . . . .     QGPL        Name, *LIBL, *CURLIB
Document password  . . . . . . .   *SAME         Name, *SAME, *NONE

                                                                   More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Hot Tip!

Limited Users cannot Change Initial Pgm, or Menu

 15

CHGPRF – Set to *PUBLIC AUT(*EXCLUDE) using GRTOBJAUT or EDTOBJAUT

```
                          Change Profile (CHGPRF)

Type choices, press Enter.

Message queue  . . . . . . . . .   DANRIEHL      Name, *SAME, *USRPRF
  Library  . . . . . . . . . . .     QUSRSYS     Name, *LIBL, *CURLIB
Delivery . . . . . . . . . . . .   *NOTIFY       *SAME, *NOTIFY, *BREAK...
Severity code filter . . . . . .   0              0-99, *SAME
Print device . . . . . . . . . .   *WRKSTN       Name, *SAME, *WRKSTN, *SYSVAL
Output queue . . . . . . . . . .   *WRKSTN       Name, *SAME, *WRKSTN, *DEV
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Attention program  . . . . . . .   *SYSVAL       Name, *SAME, *NONE...
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Sort sequence  . . . . . . . . .   *SYSVAL       Name, *SAME, *SYSVAL, *HEX...
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Language ID  . . . . . . . . . .   *SYSVAL       *SAME, *SYSVAL...
Country or region ID . . . . . .   *SYSVAL       *SAME, *SYSVAL...
Coded character set ID . . . . .   *SYSVAL       *SAME, *SYSVAL, *HEX...
Character identifier control . .   *SYSVAL       *SAME, *SYSVAL, *DEVD...
```

```
                          Change Profile (CHGPRF)

Type choices, press Enter.

Locale job attributes  . . . . .   *SYSVAL       *SAME, *SYSVAL, *NONE...
                 + for more values
Locale . . . . . . . . . . . . .   *SAME

User options . . . . . . . . . .   *NONE         *SAME, *NONE, *CLKWD...
                 + for more values
Home directory . . . . . . . . .   *SAME
```

 16

Common Misconceptions

User Limited Capabilities

www.SecureMyi.com

User Limited Capabilities

- System users can gain access to a Command Line through Various IBM supplied screens
  - From Operational Assistant Menu (ATTN Program)
    - WRKSPLF – Work with Spooled Files – My Reports
    - WRKUSRJOB – Work with User Jobs - My Jobs
  - Most IBM Supplied Menus (e.g. GO MAIN, GO USER)
- Danger in Ad-Hoc End User CL Commands
  - DLTF CUSTOMER - Delete Customer File
  - WRKACTJOB – Work with Active Jobs
- CRTUSRPRF CSMITH … LMTCPB(*YES)
  - **Impose restriction on running commands at the command line**

www.SecureMyi.com

18

User Limited Capabilities

- CRTUSRPRF CSMITH … LMTCPB(*YES)

Common Misconception

Users that are LMTCPB(*YES)
CANNOT RUN CL COMMANDS

Or rather, CANNOT RUN CL COMMANDS Ad Hoc

DLTF MYFILE

www.SecureMyi.com

19

Reality of Limited Capabilities

- **Limited Capabilities Users**
  - CAN RUN certain commands at the command line
    - **Sign off (SIGNOFF)**
    - **Send message (SNDMSG)**
    - **Display messages (DSPMSG)**
    - **Display job (DSPJOB)**
    - **Display job log (DSPJOBLOG)**
    - **Work with Messages (WRKMSG)**
  - Any CL command can be changed to Allow Limited Users to Run the Command at a Command line (Command Attribute ALWLMTUSR)

    CHGCMD CMD(WRKSPLF) ALWLMTUSR(*YES)
  - Software vendors often ship you CL Commands that are Allowed!

www.SecureMyi.com

20

Reality of Limited Capabilities

- The IBM i Access RMTCMD.exe ignores LMTCPB
- The RMTCMD.exe is an integral part of IBM i Access

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Dan Riehl>  RMTCMD  CRTLIB  HACKER

IBM i Access for Windows
Version 7  Release 1  Level 0
Submit Remote Command
(C) Copyright IBM Corporation and Others 1984, 2010.  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

Library HACKER Created
```

www.SecureMyi.com

21

Limited Capabilities Exposures

- What happens when we combine the RMTCMD exposure with User Special Authorities, like the ubiquitous *JOBCTL

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Dan Riehl>  RMTCMD  ENDSBS QINTER

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

Subsystem QINTER ending in process
```

- So, Bubba on the loading dock just shut down your system

Need Network Exit Point programs

22

Reality of Limited Capabilities

End Users CAN RUN CL commands, even with limited capabilities.

- Allowed CL Commands at a Command Line(**What is Allowed????**)
- ODBC - SQL **CALL QCMDEXC ('DLTF MYFILE' 11)**
- RMTCMD.EXE **RMTCMD DLTF MYFILE**
- IBM i Navigator **Run Command** (Uses RMTCMD)
- **Fix by Controlling RMTCMD with Network Exit Programs**
- **Determine which commands on your system are Allowed.**
- The SecureMyi Newsletter CL Command **WRKCMDSEC** does this for you.
  http://www.securemyi.com/nl/articles/cmdsec.html

www.SecureMyi.com

23

Common Misconception

The User Class Determines how Powerful a User Is

www.SecureMyi.com

The User Class Attribute

- **Does not specify what special Authorities a User has**
- **Used to determine which menu options are shown on IBM supplied menus,**
  and optionally to provide *default special authorities*
- **Default Special Authorities (Security Level 30 and Higher)**
  *USER – NO special authorities
  *SYSOPR – *JOBCTL, *SAVSYS
  *PGMR – NO special authorities
  *SECADM – *SECADM
  *SECOFR – ALL 8 special authorities

User Special Authorities

- **User profiles can be assigned special authorities**
  - *ALLOBJ – allows access to all resource on the system
  - *SECADM – ability to manage user profiles
  - *JOBCTL – control all jobs and IPL the system
  - *SPLCTL – control all spool files, and jobs in job queues
  - *SAVSYS – ability to save and restore any object
  - *SERVICE – ability to run STRSST command
  - *AUDIT – control all system auditing functions
  - *IOSYSCFG – configure system communications
- **See Article "Common Misconceptions on IBM i User Class - *SECOFR"**

http://www.securemyi.com/nl/articles/userclass.html

Common Misconceptions

On User Profile Ownership and Authority to User Profiles

www.SecureMyi.com

Ownership and Authority to User Profiles

Common Misconception

Ownership of User profiles is not a significant security related item. They can be owned by anyone. (Bill, Tom, Mary, Jenny)

*Public and Private Authority to User Profiles is not a big deal that needs any attention.

www.SecureMyi.com

28

Ownership and Authority to User Profiles

- **Ownership**
  - User Profiles, as all other objects, are owned by the Creator or the Profile, or by the Creator's Primary Group Profile
- **Authority**
  - Owner of a User Profile has *ALL authority to the Profile
  - Unless specified otherwise, User Profiles are created with *PUBLIC AUT(*EXCLUDE)

    CRTUSRPRF USRPRF(MYUSER) … AUT(*EXCLUDE)
  - User Profiles are never created with any Private authorities

www.SecureMyi.com

29

Reality of Ownership and Authority to User Profiles

- **If you have at least *USE authority to a User Profile, you can assume the identity of that User to perform unsanctioned tasks, without knowing the User's password. Breaking Segregation of Duties Policy.**
- Too many User Profiles provide *USE or higher authority to the Owner and *PUBLIC and through excessive Private Authorities.
- Software Vendors OFTEN ship Powerful User Profiles(*ALLOBJ) that are *PUBLIC(*CHANGE or *ALL)

www.SecureMyi.com

30

Reality of Ownership and Authority to User Profiles

- **Exploiting the User Profile Authorization Exposure**
- If you have *USE rights or more to another User Profile, you can run batch jobs(SBMJOB) as that user, or schedule jobs(ADDJOBSCDE) to run under that user profile.

```
SBMJOB  CMD(CHGUSRPRF  USRPRF(DANR)        +
            SPCAUT(*ALLOBJ *SECADM *JOBCTL *SERVICE))  +
        USER(POWERUSER)
```

- Running this command will give me everything needed to rule the entire system. It submits a batch job that runs under the **POWERUSER** profile, and assigns me the Special Authorities, including *ALLOBJ.
- **We incorrectly provide elevated authority to Data and Services through User Profile Ownership and through excessive *PUBLIC and Private authorities.**

www.SecureMyi.com

31

Reality of Ownership and Authority to User Profiles

- **Exploiting the User Profile Authorization Exposure**
- If you have *USE rights or higher to an application User Profile, you can run any job that User can run, and access any file, as that User.

```
SBMJOB  CMD(RUNQRY   QRYFILE( PAYROLL/PAYFILE   ))  +
        USER(PAYUSER)
```

- I have just listed out the entire content of the secured Payroll Master File
- If you have *USE or higher authority to another User profile, you can use the User Profile SWAP APIs to swap to another profile without supplying a Password.
- The command line restriction of LMTCPB is NO protection. The SBMJOB command can be run using RMTCMD.exe.

www.SecureMyi.com

32

Recommendations

- Check the authorizations on your user profiles. The following command will list out all the *PUBLIC and Private authorities of your user profiles. All Profiles should be **PUBLIC AUT(*EXCLUDE)** and have no private authorities(except groups).

PRTPVTAUT OBJTYPE(*USRPRF)

If you see user profiles listed in the resulting report with *PUBLIC *USE or greater authority, **YOU HAVE THE EXPOSURE**!

- To list ONLY User profiles that provide *PUBLIC access, use the command:

PRTPUBAUT OBJTYPE(*USRPRF)

- Set all User Profiles to *PUBLIC AUT(*EXCLUDE) **(Test! Test! Test!)**
- Change the owner of all Non-IBM supplied user profiles to QSECOFR, and revoke the current owner's authority.
- Contact software vendors for changing their profile Owners and AUT(*EXCLUDE)
- Implement an exit program to change the owner of all newly created User Profiles to QSECOFR. (SecureMyi Security Newsletter - Command **CRTPRFEXIT**)

http://www.securemyi.com/nl/articles/crtprfexit.html

www.SecureMyi.com 33

Common Misconceptions

Misconceptions about Object Authority when using Authorization Lists

www.SecureMyi.com

Authorization Lists *AUTL

- **Authorization List Defined**
  - An Authorization List is a list of *PUBLIC and Private Authorities that can be used as a template for assigning similar authorities to multiple objects
- **Typical Use of Authorization List**
  - Secure all files in a Library to one Group Profile for *USE(Read Only), and another Group Profile for *CHANGE(Update), and all others, *PUBLIC AUT(*EXCLUDE).

www.SecureMyi.com

35

Misconceptions Of Authorization Lists

Misconceptions

- When an *AUTL is assigned to an Object, all authorizations to the Object are stored in the *AUTL.
- *PUBLIC Authority to the objects secured by the *AUTL will always be determined from the *AUTL.
- *AUTL Ownership is not significant

www.SecureMyi.com

36

Reality of *AUTL

```
                         Display Authorization List

Object . . . . . . . :   PRODLIB_O       Owner  . . . . . . . :   PAYUSER
  Library  . . . . . :     QSYS           Primary group  . . . :   *NONE

              Object
User         Authority
*PUBLIC      *EXCLUDE
PAYUSER      *ALL                    Effective Authorities
GROUP_IT     *USE
GROUP_OPS    *USE
QPGMR        *CHANGE
```

```
                         Display Object Authority

Object . . . . . . . :   CSCSTP          Owner  . . . . . . . :   BOBTHETECH
  Library  . . . . . :     PRODLIB       Primary group  . . . :   *NONE
Object type  . . . . :   *FILE           ASP device . . . . . :   *SYSBAS

Object secured by authorization list  . . . . . . . . . . . . :   PRODLIB_O

                        Object
User        Group      Authority
*PUBLIC                *CHANGE          Effective Authorities
BOBTHETECH             *ALL
GROUP_IT               *ALL
GROUP_OPS              *CHANGE
QPGMR                  *ALL
```

Reality of *AUTL

```
                         Display Authorization List

Object . . . . . . . :   PRODLIB_O       Owner  . . . . . . . :   PAYUSER
  Library  . . . . . :     QSYS           Primary group  . . . :   *NONE

              Object
User         Authority
*PUBLIC      *EXCLUDE
PAYUSER      *ALL                    Effective Authorities
GROUP_IT     *USE
GROUP_OPS    *USE
QPGMR        *CHANGE
```

```
                         Display Object Authority

Object . . . . . . . :   CSCSTP          Owner  . . . . . . . :   PAYUSER Was BOBTHETECH
  Library  . . . . . :     PRODLIB       Primary group  . . . :   *NONE
Object type  . . . . :   *FILE           ASP device . . . . . :   *SYSBAS

Object secured by authorization list  . . . . . . . . . . . . :   PRODLIB_O

                        Object
User        Group      Authority
*PUBLIC                *AUTL    Was *CHANGE
PAYUSER                *ALL                Effective Authorities

Removed all Private Authorities
```

Reality of *AUTL - Fixing it!

- For the *AUTL to set the *PUBLIC authority for the objects secured by the list, the object *PUBLIC authority must be set to the value *AUTL
- Object and *AUTL ownership is critical and must not convey improper *ALL authority(Use an Owner Profile, PRODOWNER)
- Remove all Private Authorities from the Objects
- Conflicting Authorities are resolved based upon the system's authority checking order
  - User specified in Object
  - User specified in *AUTL
  - Group specified in Object
  - Group specified in *AUTL

www.SecureMyi.com

39

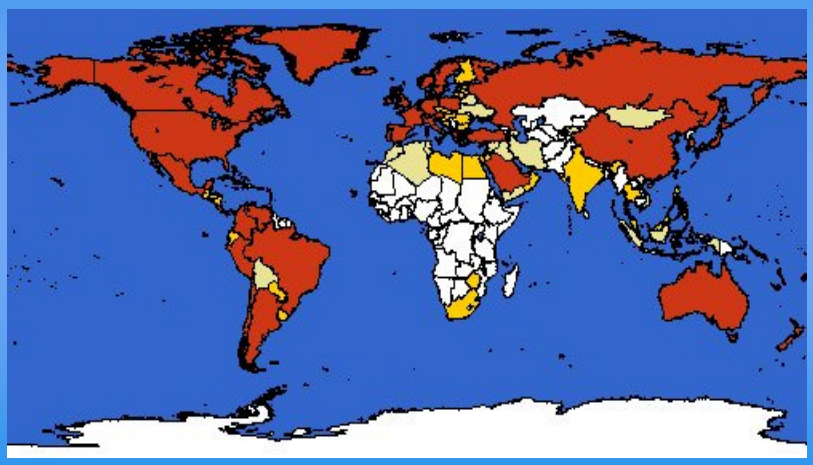
Common Misconception

IBM i is not Vulnerable to Virus, Worms or other Malware?

www.SecureMyi.com

Global Virus Map

- More than 1,000 Active Viruses (30 days)



www.SecureMyi.com

41

Virus, Worm and Malware

Common Misconception

The IBM i is not susceptible to any type of PC Virus, Worm or Malware

"We don't Need to Stinkin' Virus Protection"

www.SecureMyi.com

42

Virus, Worms, Malware?

IBM Technical Document #19541539
Viruses, the Operating System, and the Integrated File System

"The operating system is not susceptible to PC virus attacks. Viruses attack a specific computer architecture. The architecture of the IBM System i makes it highly unlikely that a virus could be written to attack it. PC-based viruses will not infect (or run on) the operating system."

www.SecureMyi.com

43

Reality of Virus, Worms Malware

IBM Technical Document #19541539
Viruses, the Operating System, and the Integrated File System

"Although the operating system can not be infected by a PC virus, if the Integrated File System on the operating system is used as a file server for PC files, the files stored on the Integrated File System may carry viruses. An infected file that is moved or saved from a PC to the Integrated File System and then redistributed to another PC can transmit a virus to the new PC. Likewise, if a network drive is mapped to the Integrated File System, a virus running on a PC (and which is capable of damaging files on a network drive) can damage any file stored on the Integrated File System."

www.SecureMyi.com

44

Reality of Virus, Worm Malware

- **The Main Exposures come from**
  - Shared Network Drives – NetServer
  - POP3 - Mail Server Attachments
  - Domino - Mail Server Attachments
  - Purposely transmitted to IFS via FTP
- **Yes… the IFS can be a Virus carrier that can further infect computers on the network**

www.SecureMyi.com

45

IBM Supported IFS Virus Scan

- **IBM added 2 System Values and 2 Exit Points to Support Native IFS Virus Scanning Options**
- **System Values to control IFS Scanning Environment**
  - **QSCANFS** and **QSCANFSCTL**
- **Exit Points Supported**
  - **QIBM_QP0L_SCAN_OPEN** – IFS Scan on Open Exit Point
  - **QIBM_QP0L_SCAN_CLOSE** – IFS Scan on Close Exit Point
- **IBM Business Partners**

  Integrated Native Virus Scanners

www.SecureMyi.com

46

www.SecureMyi.com

SecureMyi Security Newsletter

The Independent Source for Security for IBM i (ISeries and AS/400)

Thank you!

The SecureMyi Security Newsletter is found at

http://www.securemyi.com/nl.html

Presented by Dan Riehl

Dan.Riehl@SecureMyi.com

www.SecureMyi.com