www.SecureMyi.com

Securing Your User Profiles Against Abuse

Dan Riehl

IT Security and Compliance Group, LLC

Cilasoft Security Solutions - US Operations

dan.riehl@SecureMyi.com

Areas of Potential User Profile Abuse

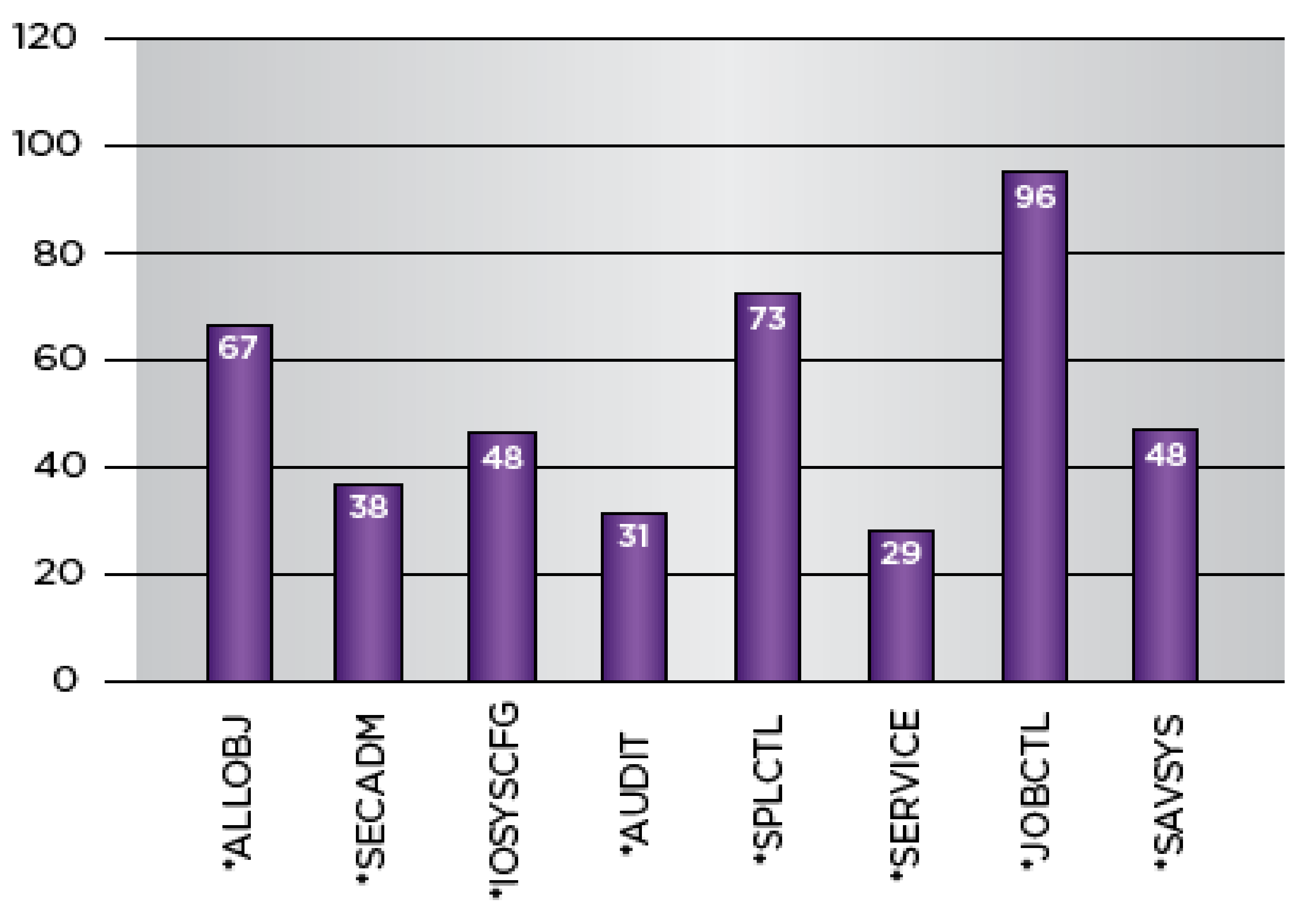
- What does a User Profile have that is open to abuse?
- Who can Abuse a User Profile?
- Password related exposures
- Limited Capabilities exposures
- Program Adoption of Authority exposures
- User Profile Authorization exposures
- Job Description *JOBD exposures

What does a User Profile have that can be abused?

- Initial program/Initial Menu
  - Provides customized end-user access to Business applications and data – Segregation of Duties?
- Special Authorities
  - *ALLOBJ, *JOBCTL, *SPLCTL, *SAVSYS, etc…
- Private Authorities
  - Libraries, Files, Programs, Commands, IFS, etc…
- Group membership
  - Special Authorities
  - Private Authorities
  - Object Primary Group

Special Authorities are Out of Control

Source Powertech: The State of System i Security 2010 (202 Systems)



Who can Abuse a User Profile?

- The actual user for which the profile is created.
  - For mischief, theft, curiosity, system disruption, etc…
  - Through various holes in security implementation
- Abused by another user, inside or outside, who hijacks the profile
  - For mischief, theft, curiosity, system disruption, etc…
  - Several methods of hijacking possible that we'll discuss

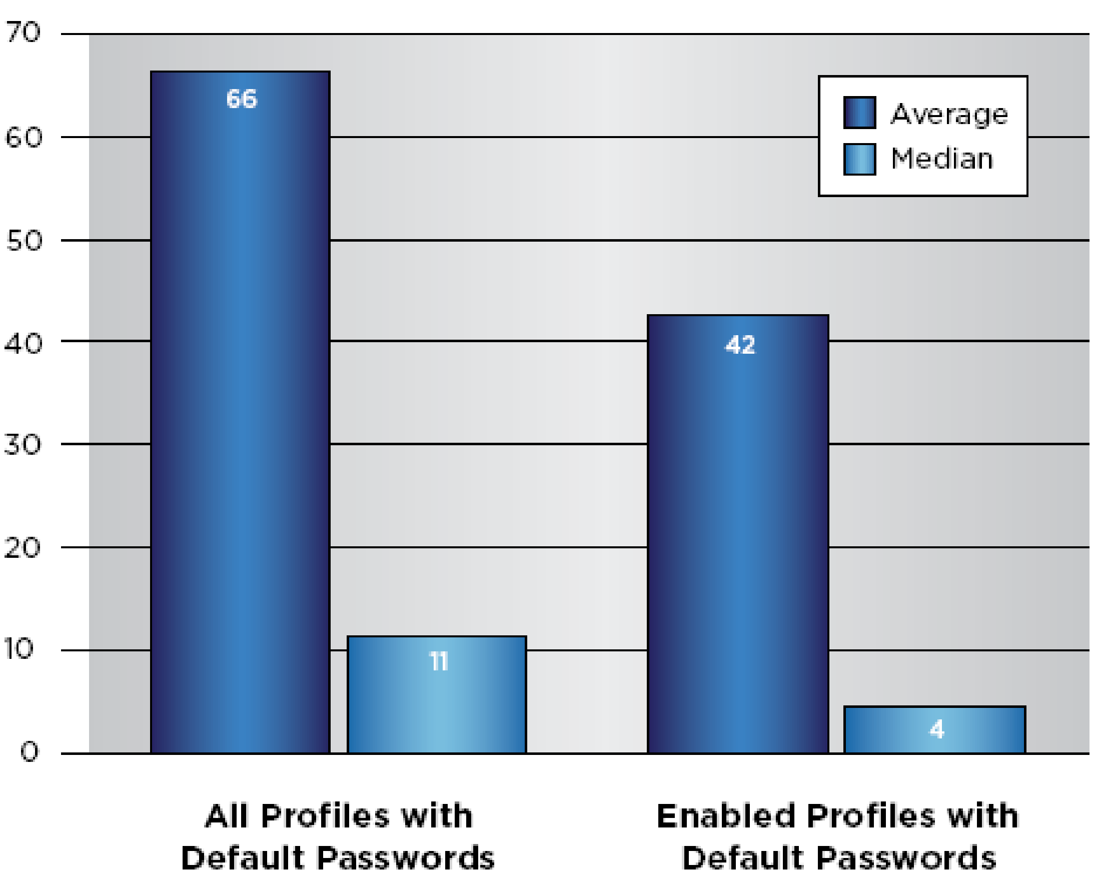
Password related exposures

- Default Passwords
  - Password = UserID
  - When creating or resetting a User Profile, don’t use the IBM default(*USRPRF) for the password. Decide on an alternate method.
- Password Sharing
  - Telling others your password
  - Writing down passwords
- Weak Password formation rules
  - Passwords like “**FLUFFY**” and “**BIGBOY**”
- Generic User Profiles
  - Several Users share the same UserID and Password
  - Commonly seen in iSeries Access and NetServer “**ABCUSER**”

Default Passwords - How many do you have?

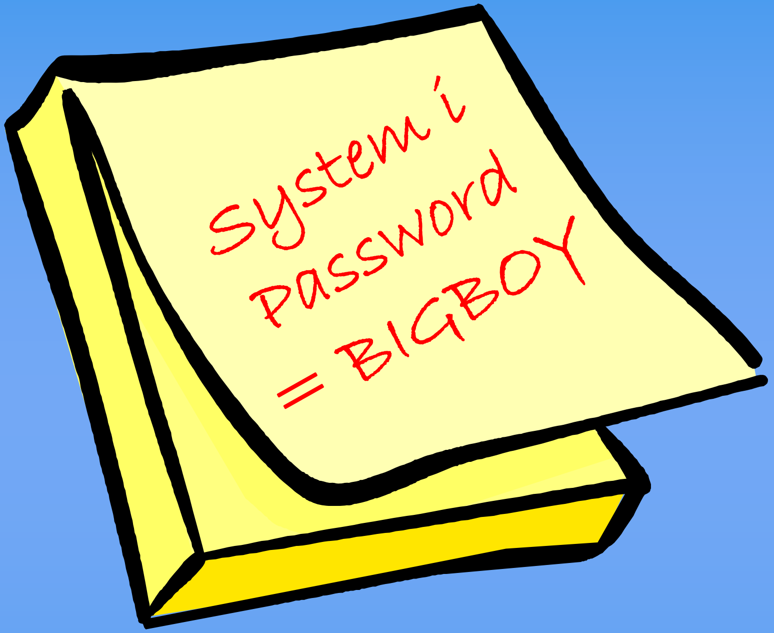
95 out of 202 systems in the study have more than 15 user profiles with default passwords.

Source Powertech: The State of System i Security 2010



Use the ANZDFTPWD command

Password Sharing



Writing down and sharing passwords with others, allows others to use and abuse your profile.

Who changed that Payroll amount?

Weak Password Formation Rules

- 58% of systems don't require a digit in passwords.
- 43% of systems do not expire passwords – meaning that a user is never forced to change their password.
- 33% of systems allow passwords to be the same as previous passwords.

The State of System i Security 2010

- This allows for Trivial Passwords that can be easily guessed
- People use pet names, spouse name, child name, favorite sports team "**DABEARS**"

If I can guess your password, I can BE YOU!

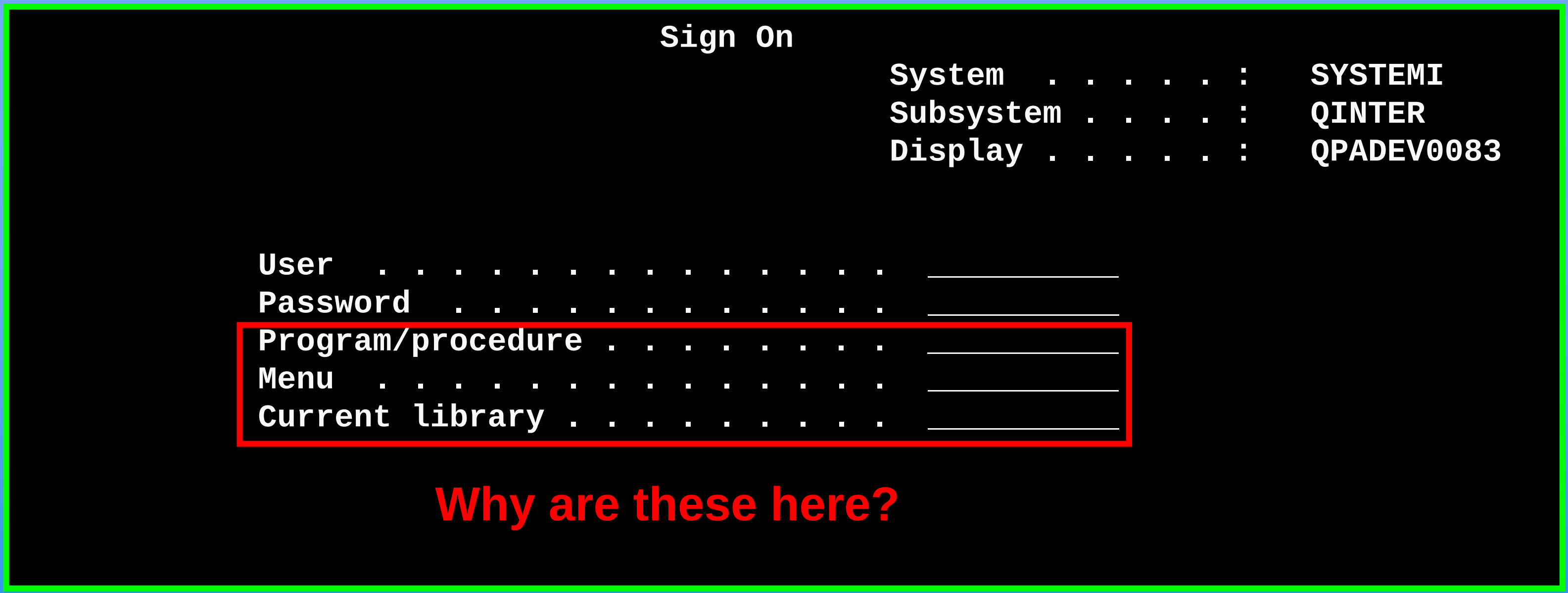
Enforce Stronger rules, and/or
consider Single Sign-on For Password Elimination

Generic/Shared User Profiles

- One user Profile and Password shared by multiple users
  - Violates most 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 used for NetServer Log-On
- Often used for the Sign-on Server Log-On
  - Very dangerous!
  - Typically means all ODBC, file transfers, all iSeries Access functions run under the generic ID (I.A. Setting - Use default UserID, prompt as needed)
  - Telnet typically does require a separate log-in, though not required
    - **QRMTSIGN System Value and Bypass Sign-on connection setting**

Limited Capabilities Exposures

- The limited capabilities attribute of a User Profile determines if the User can run ANY authorized command at a command line. It also determines whether the User can change selected values on the IBM supplied Sign-on display QDSIGNON and/or QDSIGNON2.



```
                               Sign On
                                       System  . . . . . :    SYSTEMI
                                       Subsystem . . . . :    QINTER
                                       Display . . . . . :    QPADEV0083



     User  . . . . . . . . . . . . . .   __________
     Password  . . . . . . . . . . . .   __________
     Program/procedure . . . . . . . .   __________
     Menu  . . . . . . . . . . . . . .   __________
     Current library . . . . . . . . .   __________
```

Why are these here?

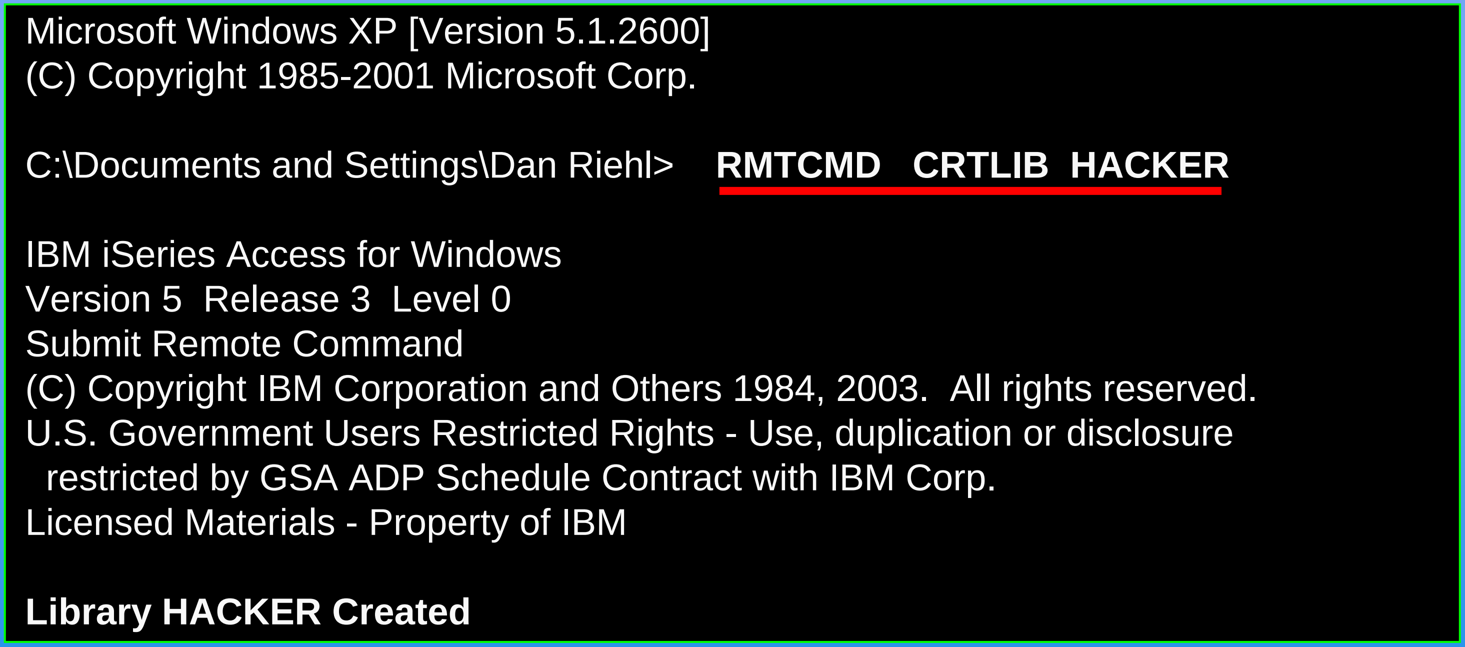
Limited Capabilities Exposures

- Limited Capabilities Users   *YES
  - Cannot change Initial Program, Initial Menu or Current Library at the Sign-on Display, or with the CHGPRF command
  - Can only use 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)**
    - **Work with Environment Variable (WRKENVVAR)**
  - To allow Limited Users to use a CL command, CHGCMD ALWLMTUSR

- Partially Limited Capabilities Users   *PARTIAL
  - Can Change Initial Menu at Sign-On or with CHGPRF
  - Can Enter Commands

Limited Capabilities Exposures

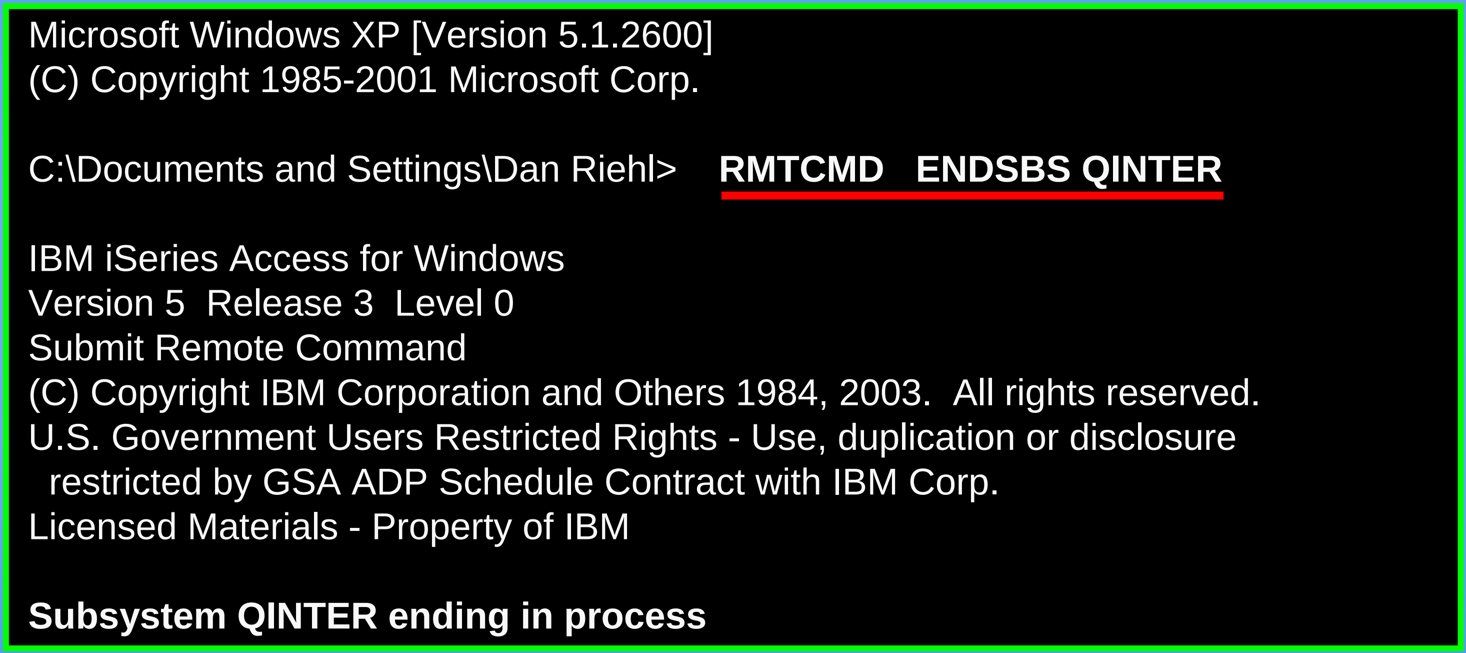
- CRTUSRPRF BOB … LMTCPB(*YES)
  - **Provides the Command Line restrictions**
  - **But, RMTCMD does not respect the LMTCPB attribute**



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

C:\Documents and Settings\Dan Riehl>   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

Library HACKER Created
```

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, Joe on the loading dock just shut down your system

Network Exit Point Software Required

Limited Capabilities exposures

Some methods to run commands, even with limited capabilities.

- ODBC - SQL **CALL QCMDEXC (‘DLTF MYFILE’ 11)**
- RMTCMD.EXE **RMTCMD ENDSBS QINTER**
- FTP RCMD V4R5 and earlier **QUOTE RCMD DLTF MYFILE**
- iSeries Navigator/Director Command Execution (Often uses RMTCMD)
- Other standard REXEC Clients

Abuse through Adoption of Authority

- Adopted authority allows the user who runs a specially modified program to temporarily borrow the private and special authorities of a more powerful user profile. In effect, becoming as powerful as the adopted user profile.
- This feature allows for implementing tighter security controls for User Profiles
  - Example: In order to reset a user’s password, the help desk/operator needs *ALLOBJ and *SECADM special authority
    - **Option 1 - Assign these powerful special authorities to the help desk/operators**
    - **Option 2 – Provide a special program that allows the help desk/operators to adopt the special authorities for the sole purpose of resetting a password**

Abuse through Adoption of Authority

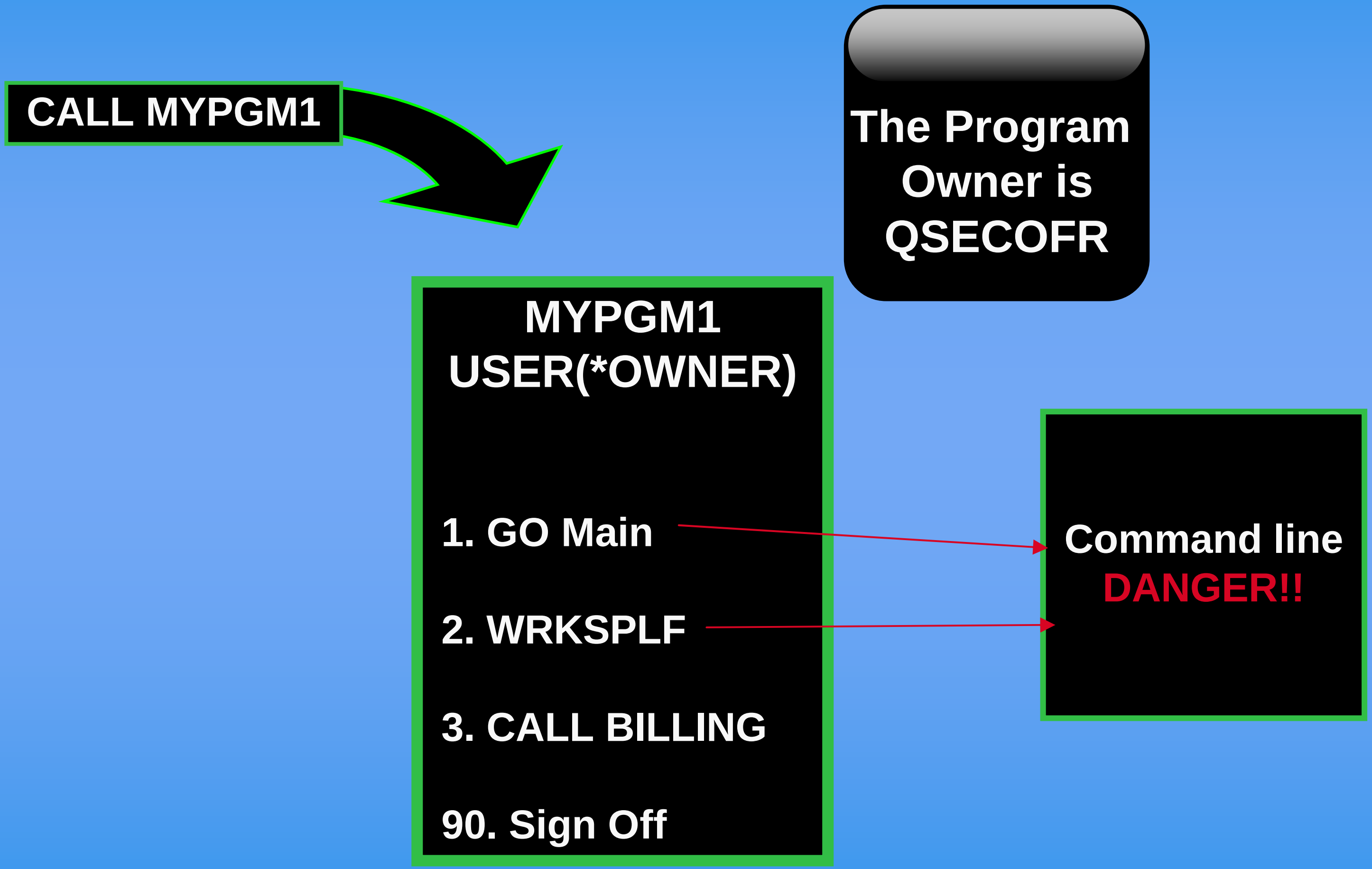
- Adopted Authority must be strictly controlled
  - Only provide *USE authority to the program for authorized users of the program

- Making a program adopt the owner's authority

CRTCLPGM MYPGM … USRPRF(*OWNER)

or, **CHGPGM MYPGM … USRPRF(*OWNER)**

Adoption of Authority – How it Works



CALL MYPGM1

The Program Owner is QSECOFR

MYPGM1
USER(*OWNER)

1. GO Main

2. WRKSPLF

3. CALL BILLING

90. Sign Off

Command line
DANGER!!

Find these programs using the command DSPPGMADP or PRTADPOBJ

Security and Adopted Authority

- Adopted Authority - Key Security Concept

Prevent Command Line access when adopted authority is in effect!

©2009 IT Security and Compliance Group, LLC
www.SecureMyi.com

Adopted Authority Back Door Programs

- The simple backdoor CL program

```
PGM
CALL QCMD
ENDPGM
```

- If this code is compiled and the program is owned by QSECOFR and it adopts authority, it provides the user with QSECOFR rights at a command line.

- Find these rogue programs using the command DSPPGMADP or PRTADPOBJ

Finding Rogue Adopting Programs

- Finding Rogue Adopting Programs
  - May be intentional, may be accidental
- Use the IBM Supplied commands
- DSPPGMADP or PRTADPOBJ

```
DSPPGMADP USRPRF(QSECOFR) OUTPUT(*PRINT)
```

  - Allows for one user at a time, but does allow output to an *Outfile

```
PRTADPOBJ USRPRF(QSECOFR,  SEC*, *ALL)
```

  - Allows for one user, a generic name as in SEC*, or *ALL
  - Limited to Printed output, but has ‘What’s Changed?’ Reporting
- Use Commercial Software
  - Commercial Software Products – In the Expo

Adopted Authority Back Door Programs

- In addition to getting *ALLOBJ power using adopted authority, you can also adopt an application owner profile for abuse.

```
PGM
CALL PAYMENU
ENDPGM
```

- In this case, the program can be owned by, and adopt APPOWNER. This potentially allows all access to the production business application.

User Profile Authorization Exposure

VERY DANGEROUS AND UBIQUITOUS VULNERABILITY

CRTUSRPRF POWERUSER … AUT(*USE, *CHANGE, *ALL)

- Allows anyone on the system to assume the identity of POWERUSER to perform unauthorized tasks. *Without knowing POWERUSER'S Password.*

- If a user profile provides *USE rights or more to other user profiles, the other user may use that profile *without knowing the password*.

Exploiting the User Profile Authorization Exposure

- If you have *USE rights or more to another User Profile object, you can easily run batch jobs as that user, or schedule jobs to run under that user profile.

```
SBMJOB  CMD(CHGUSRPRF  USRPRF(DAN)         +
                    SPCAUT(*ALLOBJ))  +
        USER(POWERUSER)
```

- Running this command will give me everything I need to rule the entire system. It submits a batch job that runs under the POWERUSER profile, and assigns me the i/OS Special Authority *ALLOBJ.

- The command line restriction LMTCPB is NO protection. The SBMJOB command can be run from RMTCMD.exe.

Exploiting the User Profile Authorization Exposure

- If you have *USE rights or more to another User Profile Object, you can use IBM Supplied APIs to swap your current job to run under the other profile. This swapped-to user then becomes the “Current User” of a job,
- These SWAP APIs are IBM supplied programs **QSYGETPH** and **QWTSETP**, and are documented at the IBM iSeries Information Center.

Do you have this exposure?

- Some VERY WELL KNOWN System i software vendors provide *SECOFR class profiles that have *PUBLIC AUT(*ALL) or AUT(*CHANGE). These allow anyone a back door to unlimited power.

- Check the authorizations on your user profiles. The following commands will list out all the *PUBLIC and Private authorities of your user profiles. All Profiles should be PUBLIC AUT(*EXCLUDE).

PRTPVTAUT OBJTYPE(*USRPRF)

PRTPUBAUT OBJTYPE(*USRPRF)

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

Note: When IT Staff members own user profiles, they have *ALL authority to those profiles.

Abuse through a Job Description

- A job description *JOBD is used as a template for running a job
- The template contains many job attributes
  - LOGLVL, JOBQ, RTGDTA, USER
- The **USER** attribute is usually set to ***RQD**, meaning a user is required, and retrieved from the user profile running the job.
- However, the USER attribute may be set to a user profile, as in the case of the QBATCH job description, the USER value is shipped from IBM as QPGMR.
- This allows a job to run under the QPGMR UserID.

Abuse through a Job Description

- To use a job description, you must have *USE or greater authority to the *JOBD.
- Under Security Level 40 and 50, you must also have *USE authority or greater to the USER specified in the *JOBD
- Under level 30, you do NOT need authority to the USER, only to the *JOBD. This is one of the well publicized reasons to move past QSECURITY level 30.

Abuse Through using a Job Description

- This vulnerability is exploited mostly when submitting batch jobs.

```
SBMJOB  CMD(CHGUSRPRF  USRPRF(DAN)
                       SPCAUT(*ALLOBJ))
        JOBD(POWERJOBD)
        USER(*JOBD)
```

- If you are Security level 30, You have this problem…
- Solution…. Move to QSECURITY Level 40 or 50

RECAP

- Password related exposures
- Limited Capabilities exposures
- Program Adoption of Authority exposures
- User Profile Authorization exposures
- Job Description *JOBD exposures

www.SecureMyi.com

Secure Your System i

Thank you!

Dan Riehl
dan.riehl@SecureMyi.com

www,Cilasoft.com