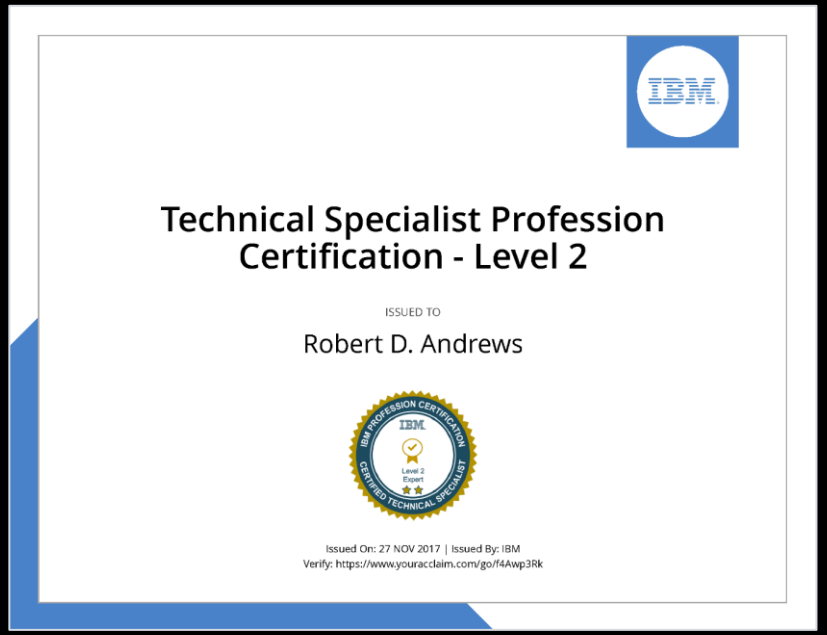
IBM i Administrative Security Risks

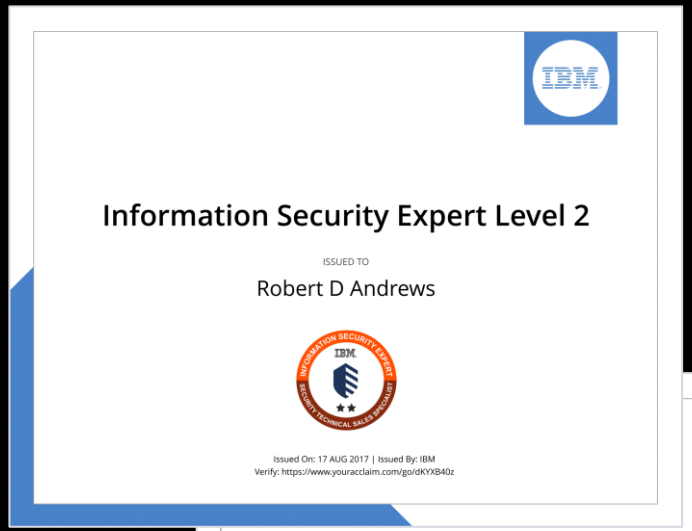
Robert D. Andrews
Senior Managing Security Consultant
IBM Systems Lab Services
robert.andrews@us.ibm.com

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Certifications





Background and Basics

“You cannot **prove security**.

You can only **prove insecurity**.”

Security vs. Secure vs. Securable

Security is the quality or state of being secure

Secure means to be protected from risk of potential harm or danger

- Trying to understand the risk and deal with it appropriately
- Risk can be: Accepted, Avoided, Transferred, or Reduced / Mitigated

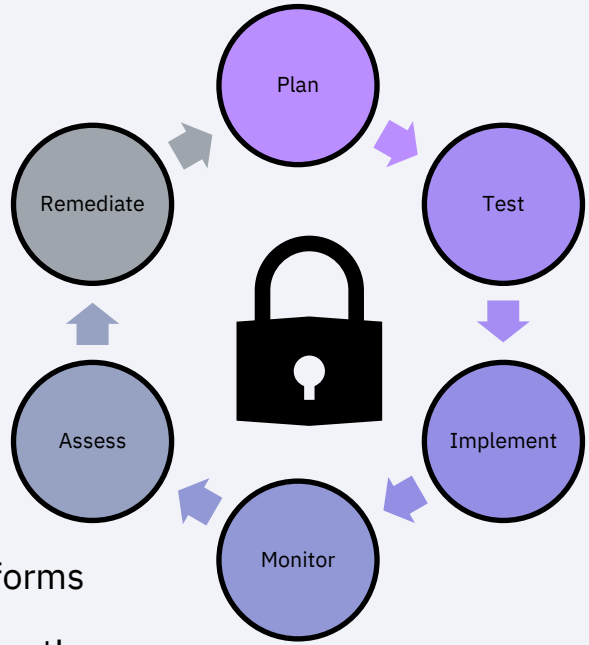
Securability goes to the degree at which something is able to be secured

- The IBM i is highly securable, if you set it up correctly!

Company's should have an overall IT Risk policy – platform agnostic

- That policy should then have technical implementation plans for all platforms

Security is a cycle: Plan, Test, Implement, Monitor, Assess, Remediate, Repeat!

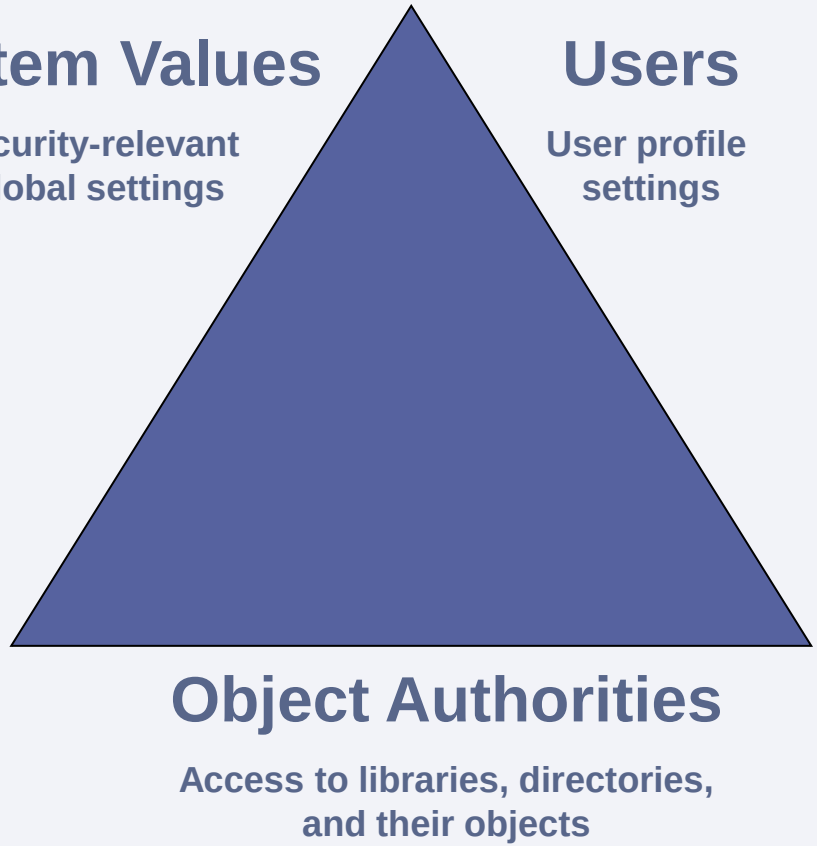


The Security Triangle

The IBM i Security model is based on the Security Triangle:

- System Values
- User Profiles
- Object Authorities

All three parts are key to understanding a system's true security posture



System Values

For every System Value (158 on 7.4), have a documented expected value

- Review these settings on all LPARs – production and dev / test

Focus on Security related System Values (48 on 7.4)

- QSECURITY is most important – should be at 50 (40 minimum)
  - Can use “Pseudo” mode to test system before going to level 40 if below
    - See the “Changing to security level 40” section of the Security Reference
- Use QPWDLVL 3 and QPWDRULES for enhanced password controls
- Use the electronic lock in SST to prevent changes to these system values

System Auditing

The IBM i has robust auditing capabilities built-in – Turn them ON!

Use Change Security Auditing (CHGSECAUD) command to set them up

IBM Recommends:

- QAUDCTL at: *AUDLVL, *OBJAUD, and *NOQTEMP
- QAUDLVL at: *AUTFAIL, *OBJMGT, *PGMFAIL, *SAVRST, *SERVICE, *SECURITY, and *SYSMGT
- Be careful with “noisy” options (*CREATE, *DELETE, *JOBDTA, *PRTDTA, *SPLFDTA)
  - Don’t want to hide the important messages in a huge pile of hay!

Do not put your Audit Journal Receivers in QSYS or QGPL – use their own secured library

Use command auditing to record the actions of privileged users – CHGUSRAUD AUDLVL(*CMD)

Integrate with a central SIEM (Splunk, QRadar, ArcSight) using the Syslog Reporting Manager

Patches

As with all Operating Systems, make sure you keep your IBM i current on patches

IBM recommends applying patches at least quarterly

Make sure to get current:

- Technology Refresh
- Cumulative PTF
- Group HIPER (High Impact and Pervasive)
- Group Security
- Db2 for IBM i
- Any other IBM, BP, vendor, or open source applications used

Major Risks

Special Authorities

The IBM i has eight (8) Special Authorities that grant administrative rights to profiles

These special authorities are special! Each brings a set of risk to the system

Limit them each to ten (10) or fewer users regardless of system size

- Limited to the true owners of the system
- Don’t forget group expansion

We often see 90%+ of the users on a system have *JOBCTL or *SPLCTL

- What’s the risk introduced?

Rumor: It is safe to give a user *ALLOBJ as long as you do not give them *SECADM as well

FALSE!! An *ALLOBJ user can do anything, including giving themselves *SECADM

Special Authorities Defined

*ALLOBJ – allows a user authority to perform all operations on all objects

- You cannot prevent an *ALLOBJ user from accessing an object

*AUDIT – allows a user to define the auditing characteristics of the system, objects, and users

*IOSYSCFG – allows a user to configure communication and input/output devices on the system

*JOBCTL – allows a user to control jobs on the system

*SAVSYS – allows a user to save and restore objects

*SECADM – allows a user to work with user profiles on the system

*SERVICE – allows a user to perform software service functions on the system

*SPLCTL – allows a user unrestricted control of output queues on the system

Special Authority Risks – What's the worst that could happen?

*AUDIT – can turn off auditing, remove logs from system

*IOSYSCFG – can change network configurations, disable network access

*JOBCTL – can change or cancel any job on the system, put system in restricted state, IPL system, affect performance (WM lockup)

*SAVSYS – save ANY file, view any tape, save object storage freed

*SECADM – can create back door profiles, boost others authority

*SERVICE – can access SST (System Service Tools), run advanced analysis macros, Display/Alter/Dump (D/A/D) any storage

*SPLCTL – can access ANY spool file (printer output), even confidential ones

*ALLOBJ – CAN. DO. ANYTHING. PERIOD.

User Profile Passwords

User Profiles are secured by a password, used on all interfaces

Use strong password rules – IBM Recommends:

- Password level 3, require any 3 different character types (lower, upper, numeric, special), minimum length 16, maximum length 128, password expiration 90 days, password change block of 24 hours, require difference of last 32 passwords, limit profile in password, and enforce rules on all create and change interfaces

Consider Multi Factor Authentication (MFA) or Single Sign On (SSO) / Kerberos to secure your IBM i – tools available from IBM and Security BP's

Don't forget your System Service Tool's (SST) password settings as well!

- New Display SST Security Attributes (DSPSSTSECA) command at 7.4

Default and Dictionary Passwords

Do not use default passwords (where the password matches the user profile) when creating new accounts

- Change the default on CRTUSRPRF to PASSWORD(*NONE)
- Use a randomly generated password for each new user account

Do not use allow users to set easy to guess or well-known (dictionary) passwords like ABC123 or PASSWORD

- Use the QIBM_QSY_CHK_PASSWRD Exit Point to check candidate passwords against password dictionaries – easily available online
- Can be self written or tools available from IBM and Security BP’s

Remember, administrator accounts are some of the most powerful and often weakest secured accounts on a system – are you bypassing security controls?

*PUBLIC Objects

Users should only be given authority to the objects they need to do their jobs +

All objects have a *PUBLIC authority attribute = *PUBLIC should be *NONE

This is especially true for user profile and library objects! Why?

If a user profile has *PUBLIC *USE or higher, anyone can use its authority!

- Including any special authorities
- Submit work or do tasks under the other profile to mask their true identity

Check for *PUBLIC user profiles with PRTPUBAUT OBJTYPE(*USRPRF)

- The OS has 3 public profiles – do not alter: QDBSHR, QDBSHRDO, QTMPLPD
- Any other profile that comes up should be reviewed and corrected

*PUBLIC Objects

If a library has *PUBLIC *USE or higher, anyone can start looking inside of it

- Libraries are like hallways, if blocked, all doors regardless of state are also blocked!

If a Library has *PUBLIC *CHANGE, anyone can create objects into it

- This is often the case coming from QCRTAUT system value default being *CHANGE
- What happens if this library is above QSYS in the System Library List?

If a Library has *PUBLIC *ALL, anyone could potentially do anything, even delete it!

- Assuming all objects in it also picked up *PUBLIC *ALL on create

Besides libraries, consider other key object types like Subsystems, Job Descriptions, Job Queues, and Authorization Lists

DDM / DRDA Password Requirements

Distributed Data Management (DDM) and Distributed Relational Database Architecture (DRDA) provide remote access to your IBM i

By default, this is secured requiring both a user profile and password to connect

However, many apps (BRMS and HA apps like MIMIX, iTERA, QuickEDD, etc.) often instruct the administrators to turn off password checking

- Makes setting up cross-system communications very simple!
- However, also allows anyone to connect as any user profile by just knowing its name
  - Including powerful accounts such as QSECOFR

Must check Change DDM TCP/IP Attributes (CHGDDMTCPA) to see what your password requirements are (want *YES / *USRIDPWD or *ENCRYPTED / *USRENCPWD)

- If *NO / *USRID (user id only) you are at great risk!!

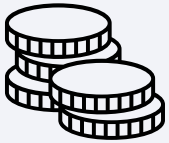
Hacking DDM and DRDA

Connect as QSECOFR / no password, create an admin account, then log in anywhere with new user

1. DDM – Submit Remote Command
- ADDSVRAUTE USRPRF(*CURRENT) SERVER(QDDMSERVER) USRID(QSECOFR) PASSWORD(*NONE)
- Submit Remote Command (SBMRMTCMD) to create an admin account with a password
2. DRDA – Start SQL Interactive Session (STRSQL)
- CONNECT TO REMOTESYS USER QSECOFR USING ‘ ’
- Call QCMDEXC to create an admin account with a password
3. DRDA – From a PC with Db2 Connect
- db2 connect to myibmi user QSECOFR using x
- Call QCMDEXC to create an admin account with a password

Ransomware

IBM i and Ransomware



Ransomware is malware (virus) that infects PCs and encrypts files to block access without paying a ransom to unlock them

- No currently known ransomware runs directly on the IBM i

Most infections come from opening email attachments or social engineering

- Test your employees and help desk staff with social engineering attacks

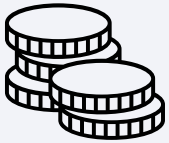
Most will not only encrypt local PC files but any connected network drives

- This is the risk to the IBM i from ransomware

Quickly isolating and disconnecting infected PCs will help save IT resources

Using a network-based file storage with versioning (multiple prior copies of files) is the best way to protect PC data

Ways to Protect your IBM i from Ransomware



Disable Guest network access – only allow authenticated users

Eliminate as many network shares as possible

Make the shares that remain as far down the directory path as possible

- Limit the amount of files exposed to the network
- Never share the root (/) of the IFS

Set the share to read only if possible

Have a complete and tested backup methodology

- Easiest way to recover from ransomware is to wipe and restore data
- Do not pay the ransom – this only encourages future attacks

Ways to Protect your IBM i IFS

Be default, the IFS Root (/) is set to *PUBLIC *RWX

- This means all users have both read and write authority to the root
- Any folders created off the root inherit these same *PUBLIC *RWX rights
- Any files created in those folders also inherit *PUBLIC *RWX rights
- You can see this quickly opens a large amount of data to be read and written to

IBM recommends changing the IFS Root (/) to *PUBLIC *RX

- This does NOT affect any existing folders or files, just newly created ones after the change
  - Can use CHGAUT with SUBTREE(*ALL) to change existing folders and files
- Please check with your third-party apps to see how they would be affected by this change

A few other bits...

Use Encryption – Both at Rest and In Flight

Secure your data at rest and in flight via encryption

- Encryption is not a “magic bullet” for security – limited effectiveness

Secure your data at rest by using SAN encryption (best option) or encrypted ASPs on the system (possible performance issues)

- Don’t forget to encrypt your tapes or other types of backup media

Secure your data in flight by using industry-standard TLS encryption

- Available for almost every interface: Telnet, FTP, ODBC / JDBC, DDM / DRDA, Host Servers, Remote Journaling, Cluster, LDAP, POP, and SMTP
- Use strong protocols (TLS 1.2 or above) and ciphers (AES or better)
- If using more modern interfaces (i.e. SSH), make sure you understand how to secure them as well – many are not IBM i native

Outside Reviews or Assessments

Have your IBM i audited/reviewed/assessed by an outside security group

Will catch items your staff are not aware of

Good to get “fresh eyes” to review your current security posture

Most security frameworks recommend an annual / once a year review

Compare prior years assessments to current assessments to see progress made (or lost)

IBM Lab Services, as well as many third-party security companies, offer these assessments

- Avoid completely free automated scans – you get what you pay for!
  - Nessus vulnerability scanner will produce MANY false positives on IBM i – worthless
- Make sure the company assessing your IBM i has knowledge in IBM i
  - If they ask you for your Root account password or use an “AS/400 Checklist” RUN!

Staffing as a Security Concern

Many IBM i shops have limited staffing for their systems

Admins often also serve as programmers, DBA's, help desk, network admins, and security staff all in one

Consider the age and seniority of your IBM i staff

- How soon will they retire? What is your continuity plan? How much is documented?

Security is a specialized role that needs dedicated resources

- And that does not mean your Windows Security person, unless they are trained in IBM i as well

Security is only as strong as its weakest link

Security is ultimately about protection – of your assets and your identity

Asking about Assistance

IBM Systems Lab Services IBM i Security Team

Security Services for IBM i include:

- Security Assessment
- Single Sign On Implementation
- Security Remediation
- Encryption Assistance
- Security Mentoring

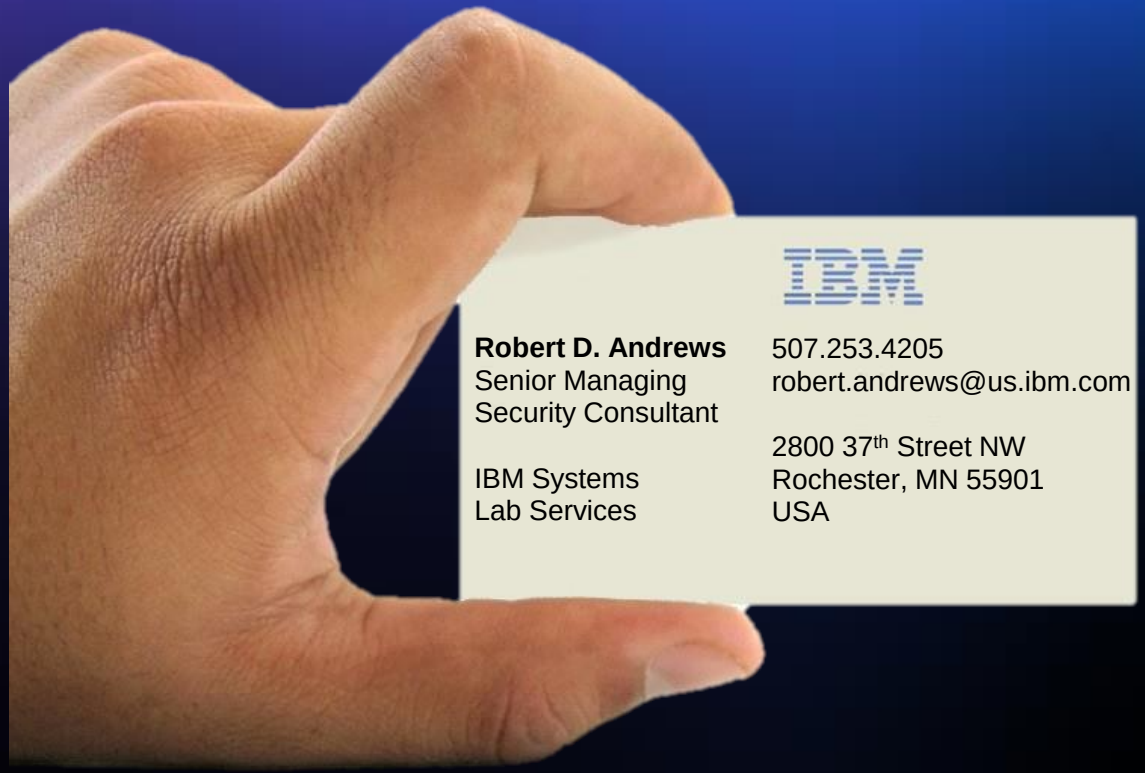
IBM Systems Lab Services:

- Simplify management and measurement of security & compliance
- Reduce the cost of security & compliance
- Improve detection and reporting of security exposures
- Improve auditing/monitoring to satisfy reporting requirements
- Guide your business toward a more secure operational model

Security and Compliance Tools for IBM i

Tool	Benefits
Compliance Automation Reporting Tool (CART)	Demonstrate adherence to pre- and customer-defined security polices, system component inventory. Centralize security management and reporting via Db2 Web Query.
Privileged Elevation Tool (Fire Call)	Ensures compliance with guidelines on privileged users.
Syslog Reporting Manager (SRM)	Simplifies sending of audit log messages to SIEMs.
Network Interface Firewall (Exit Point Tool)	Restrict access to various system services by user and connection source.
Advanced Authentication	Multifactor Authentication to secure sensitive access.
Single Sign On (SSO) Suite	Tools to assist in the complete lifecycle of a Kerberos user.
Have a need? More tools and info online at ibm.biz/IBMiSecurity	

Questions?


IBM
Robert D. Andrews
Senior Managing
Security Consultant
IBM Systems
Lab Services
507.253.4205
robert.andrews@us.ibm.com
2800 37th Street NW
Rochester, MN 55901
USA

Thank you

Follow us on:

ibm.biz/IBMiSecurity

© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.