Top Ten Security Vulnerabilities in z/OS & RACF Security

Philip Emrich
Senior Professional Services Consultant
pemrich@go2vanguard.com

9 – 14 August 2015
SHARE 125 – Session 11714
Legal Notice

Copyright

©2014 Vanguard Integrity Professionals - Nevada. All Rights Reserved. You have a limited license to view these materials for your organization's internal purposes. Any unauthorized reproduction, distribution, exhibition or use of these copyrighted materials is expressly prohibited.

Trademarks

IBM, RACF, OS/390, System z, and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. UNIX is a registered trademark of The Open Group in the United States and other countries. Linux is a registered trademark of the Linux Mark Institute in the United States and other countries. Vanguard Administrator, Vanguard Advisor, Vanguard Analyzer, and Vanguard Configuration Manager are trademarks of Vanguard Integrity Professionals – Nevada.
The Need for “Best Practices” for z/OS Security

1. This part introduces the need to assess z/OS systems for vulnerabilities and the reasons for doing regular vulnerability assessments.

Vanguard’s most Frequently Encountered Significant Exposures

2. This part covers the “Top Ten” most frequently encountered Severe or High risk exposures encountered in assessment of z/OS systems Vanguard has conducted for our clients.

Assessment and Remediation

3. This part discusses the overall assessment process and remediation of exposures identified.
The Issues

• **Is your mainframe critical to your enterprise?**
  – Is it central to your Disaster Recover Plan
  – Does it host mission critical applications and data
  – What would be the immediate and long term impact of a system outage

The level of security controls for your mainframe must be sufficient for the criticality of the data and business processes hosted on it.
System z/OS® workloads are going UP in terms of data stored and transactions processed, NOT down.

This is the opposite of the public or common perception.

“The” Critical System in your Network

If you have a z/OS system in your network, that is the “bank vault” – everything else is just an “ATM”.
The Issues

• If you have a breach or a hack on your mainframe, three things could happen:
  – Your critical data could be manipulated, stolen, or compromised
  – Your operations could become compromised
  – Your reputation could become damaged
The Invisible Mainframe

- Hundreds of Windows, Linux™ and UNIX® Servers.
- One, Two, Three, four? z/OS servers

World wide, z/OS servers are far less than 1% of servers.

2,400 Enterprises with one or more z/OS systems.
The Situation

• While most IT security teams tend to lump mainframe systems into the category of legacy systems unnecessary or impossible to scrutinize during regular audits, that couldn't be farther from the truth.

• I see them described as legacy all the time: 'Oh, we don't need to implement this policy because it's a legacy system.' Calling a mainframe legacy is like calling Windows 2012 Server legacy because parts of the Window NT kernel are still in the code. Or it's like calling my car legacy because it's still got tires.

• A website was released with a number of tools to aid with the hacking of a mainframe, including VERY SPECIFIC mainframe vulnerabilities. (ACEE zapper, USS elevated permission code, TN3270 sniffers) - https://github.com/mainframed
65% of the world’s mission critical data resides on IBM mainframes.

Ant Allan, V.P. Gartner

If an enterprise has IBM z/OS systems, 85% of their critical data is processed or stored on the IBM z/OS system.

Ant Allan, V.P. Gartner
The Mainframe is still an important platform
Security can fall short
  – Creating high-risk vulnerabilities
Fewer security guidelines than other servers

Ant Allan
Research VP

Gartner Research
Publication Date: 20 January 2010
ID Number: G00172909

Why Your IBM z/OS Mainframe May Not Be as Secure as You Think It Is and What You Can Do About It

Ant Allan

This research describes the state of z/OS mainframe platform security and sets out an action plan for enterprises to ensure that their mainframes are properly secure. The IBM z/OS mainframe continues to be an important platform for many enterprises, but security can fall short of the platform’s potential and CIOs’ and chief information security officers’ (CISOs’) expectations (without them realizing it).

Key Findings

- A real shortage of mature mainframe security skills makes configuration and administration errors more likely than on other enterprise server operating systems (OSs) in the same enterprises — and less likely to be found and remedied.
- Relatively lax compliance audits fail to identify mainframe control weaknesses, and lack of management attention can allow “worst practices” to continue. The risk of compromise has increased with greater mainframe connectivity.
- There are fewer z/OS-specific security guidelines than for other enterprise server OSs. Mainframe-specific compliance requirements are rare, but increasing.
- Full compliance with mainframe-specific security guidelines is difficult, and the incidence of high-risk vulnerabilities is astonishingly high.
The Logica and Nordea Hack

- Pirate Bay co-founder Gottfrid Svartholm Warg was charged with hacking the IBM mainframe of Logica, a Swedish IT firm that provided tax services to the Swedish government, and the IBM mainframe of the Swedish Nordea bank, according to the Swedish public prosecutor Henrik Olin.

- A large amount of data from companies and agencies was taken during the hack, according to Olin, including a large amount of personal data, such as personal identity numbers of people with protected identities.

- Only one of the attempts to transfer money from eight Nordea bank accounts succeeded, according to Olin. The intruders managed to do that by hacking the mainframe that was located in Sweden.

- They attempted to steal over $900K from Nordea customers accounts.
Top Reasons for Security Vulnerabilities

• Retirement of skilled professionals – makes it difficult to assess your own security

• Lax in audits due to insufficient skill sets – not communicated to management

• Few documented guidelines available

• Full compliance with standards and regulations is difficult
Top Gartner Recommendations

- Develop and update your policies
- Audit your mainframe, remediate vulnerabilities
- Ensure your security and risk management policies are enforced
- Invest in training and education
- Evaluate intelligent administration and auditing tools
Most people involved in IT do not remember the '70s and '80s when mainframes ruled the world. One of my first consulting projects as a student involved fixing an IBM 370 Assembler program that used registers, that is, a low-level part of the hardware architecture, as a convenient form of storage for a variable. Ah, those were the days: You programmed with the details of computer architecture in your head. They were also the days when computer science was new and shiny and not categorized only as an engineering discipline. In the late '70s the University of Michigan housed the Computer Science department in the School of Literature, Science and the Arts. I'm one of a few people with a Bachelor of Arts (not Science) in computer science. As an assistant to computer science pioneer Arthur Burks, I graded papers in a room shared with a chunk of the ENIAC, one of the first digital computers. But I digress.

My love of the complexity of all things surrounding the mainframe led me to my first job as an IBM MVS System Programmer, the rough equivalent of a system administrator. Back then, virtualization was old news; any number of different IBM operating systems could run on one machine using IBM's VM technology. Most people think the mainframe era is past, but in everyday life the credit card processors and the grids through which electricity and telecommunications flow are largely handled by mainframes.

IBM has elegantly brought mainframes forward, and today Linux runs on the computer architecture I programmed for. Various analysts report more than 15,000 mainframe installations worldwide, over half of which are at more than 1,000 million instructions per second (MIPS), with the number of MIPS still growing. David B. Black, technology partner at venture firm Oak Investments, has first-hand experience with the durability of the mainframe processing architecture from his tenure as Chief Technology Officer at credit-card processing company PaySys in the 1990s. The PaySys software based on the mainframe was sold in 2001 to market leader First Data Corporation, but the version that ran on commodity blades was not part of the deal and never grabbed a large share of market. Black points out that the logical architecture I programmed against as a student may be old, but the implementation of that architecture is just as new as any computer on the market today. "Mainframes are not implemented in vacuum tubes. The design may be old, but the hardware is state of the art," said Black. Black says mainframes are here to stay because the backward compatibility of the new hardware with the old logical architecture enables old software to run extremely well. "This old software has, one step at a time, one year at a time, encountered and solved all of the business and human issues involved in processing credit cards and many other tasks," Black points out. "How much money could you save not using a mainframe? A million dollars? Well, that sounds like a lot until you realize it's the equivalent of five or six top software engineers for a year. Could five or six top software engineers over a year even understand, much less implement, solutions created over a couple of decades by hundreds, if not thousands, of engineers? In that context, the mainframe is cheap."
Business Realities

**The Need to Implement Security “Best Practices”**

Information Security Compliance is a top organizational initiative

- Laws, Regulations, and Standards require validation of proper implementation of IT internal controls.
- IT Internal Control failures threaten the organization’s image and can carry heavy fines and even executive management imprisonment.
- Cyber-crime activities are a serious threat and companies are expected to implement all reasonable measures to prevent successful attacks.
- Outside auditors can and are issuing sanctions that restrict core business activities based on IT security risks identified in their audits.

**Bottom Line:** The Information Security organization must be proactive in their efforts to implement and maintain Security “Best Practices” in their enterprises.
Origins of “Best Practices”

- **Objective Sources:**
  - Regulatory Compliance
    - HIPAA (1996)
      - HITECH Act 2009
    - Gramm-Leach-Bliley Act – 1999 (GLBA)
      - Financial Privacy Rule
      - Safeguards Rule
    - Sarbanes-Oxley Act of 2002 (SOX)
      - Section 404: Assessment of internal control
    - PCI-DSS
      - Payment Card Industry - Data Security Standard
      - [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org)
      - PCI Standards & Documents
      - Documents Library
Origins of “Best Practices”

• Objective Sources:
  – Regulatory Compliance
    • DoD DISA STIGs
      – z/OS STIG adopted by Centers for Medicare & Medicaid Services (CMS)
    • NIST (National Institute of Standards and Technology)
      – co-hosts with DHS (Department of Homeland Security)
      – security configuration checklists on the National Vulnerability Database
        [Link: http://web.nvd.nist.gov/view/ncp/repository]
      – Target Product: IBM OS390
The identified security issues present risk to regulatory / industry compliance standards depending on the data present within the assessed system.
Origins of “Best Practices”

• Subjective Source:
  – Vanguard Best Practices
    • Professional Services Consultants with an average of 30+ years experience
    • Based on our technical understanding of z/OS and key Subsystem software
    • Related to risks and exposures identified in hundreds of Security Assessments conducted over more than 20 years
    • Security Assessments comprise several hundred tests
Vanguard's Assessment Process

• Analysis of over Hundreds of Assessments
  – Private firms across numerous industries
  – Various governmental agencies:
    • Federal
    • State
    • Local
  – Totaling over 1800 Individual Findings
  – Over 300 unique Findings
  – Correlated to regulations or compliance requirements
  – Categorized by Severity and Remediation effort
Vanguard’s Exposure Severity Rating

- **SEVERE** (needs immediate remediation)
  - Immediate unauthorized access into a system
  - Elevated authorities or attributes
  - Cause system wide outages
  - The ability to violate IBM’s Integrity Statement

- **HIGH** (needs remediation in the near future)
  - Vulnerabilities that provide a high potential of disclosing sensitive or confidential data
  - Cause a major sub-system outage
  - Assignment of excessive access to resources

- **MEDIUM** (needs a plan for remediation within a reasonable period)
  - Vulnerabilities that provide information and/or access that could potentially lead to compromise
  - The inability to produce necessary audit trails

- **LOW** (should be remediated when time and resources permit)
  - Implementation or configuration issues that have the possibility of degrading performance and/or security administration
# Top Ten z/OS Vulnerabilities

**Scope:** Vanguard Top 10 z/OS Risks Based Upon Criticality of Finding

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Vulnerability Description</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>73%</td>
<td>Excessive Number of User ID’s w/No Password Interval</td>
<td>SEVERE</td>
</tr>
<tr>
<td>60%</td>
<td>Inappropriate Usage of z/OS UNIX Superuser Privilege, UID = 0</td>
<td>SEVERE</td>
</tr>
<tr>
<td>52%</td>
<td>Data Set Profiles with UACC Greater than READ</td>
<td>SEVERE</td>
</tr>
<tr>
<td>40%</td>
<td>RACF Database is not Adequately Protected</td>
<td>SEVERE</td>
</tr>
<tr>
<td>39%</td>
<td>Excessive Access to APF Libraries</td>
<td>SEVERE</td>
</tr>
<tr>
<td>38%</td>
<td>General Resource Profiles in WARN Mode</td>
<td>SEVERE</td>
</tr>
<tr>
<td>33%</td>
<td>Production Batch Jobs have Excessive Resource Access</td>
<td>SEVERE</td>
</tr>
<tr>
<td>52%</td>
<td>Data Set Profiles with UACC of READ</td>
<td>HIGH</td>
</tr>
<tr>
<td>51%</td>
<td>Improper Use or Lack of UNIXPRIV Profiles</td>
<td>HIGH</td>
</tr>
<tr>
<td>51%</td>
<td>Started Task IDs are not Defined as PROTECTED IDs</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

**Note:** Percentage is frequency of occurrence of finding.
Data collected from hundreds of security assessments performed by Vanguard Integrity Professionals.

©2015 Vanguard Integrity Professionals, Inc. All Rights Reserved. You have a limited license to view these materials for your organization's internal purposes. Any unauthorized reproduction, distribution, exhibition or use of these copyrighted materials is expressly prohibited.
<table>
<thead>
<tr>
<th>Finding</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Excessive Number of User IDs with No Password Interval</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk - Severe</th>
</tr>
</thead>
<tbody>
<tr>
<td>User IDs with no password Interval are not required to change their passwords. Since passwords do not need to be changed periodically, people who knew a password for an ID could still access that ID even if they are no longer authorized users.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recommended Best Practice and Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review each of the personal user profiles to determine why they require NOINTERVAL. Their passwords should adhere to the company policy regarding password changes. If the user ID is being used for started tasks or surrogate, it should be reviewed and changed to PROTECTED. If the user ID is being used for off platform process, then review controls for where the passwords are stored and consider converting to usage of digital certificates or other alternatives.</td>
</tr>
</tbody>
</table>
Assessment Finding #2

Finding

Inappropriate Usage of z/OS UNIX Superuser Privilege UID(0)

Risk - Severe

User IDs with z/OS UNIX superuser authority, UID(0), have full access to all UNIX directories and files and full authority to administer z/OS UNIX.

Recommended Best Practice and Remediation

The assignment of UID(0) authority should be minimized by managing superuser privileges through profiles in the UNIXPRIV class. For those user IDs that do not require unrestricted superuser authority, but do require some privileged UNIX authority, UID(0) should be changed to a non-zero UID and access should be granted to one or more of the ‘BPX.qualifier’ profiles in the FACILITY class and/or access to one or more profiles in the UNIXPRIV class. For user IDs associated with started tasks, other than those for which UID(0) is appropriate, product documentation should be reviewed to determine what specific UNIX authority is required, grant only that authority, and then replace UID(0) in their respective OMVS segments with a non-zero value.
## Assessment Finding #3

<table>
<thead>
<tr>
<th>Finding</th>
<th>Dataset Profiles with UACC Greater than READ</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk - Severe</strong></td>
<td>Data sets that are protected by a RACF profile with a UACC greater than READ allow most users with system access to read or modify these data sets. In addition, users may be able to delete any data set covered by the dataset profiles that have a UACC of ALTER.</td>
</tr>
<tr>
<td><strong>Recommended Best Practice and Remediation</strong></td>
<td>Review each of these profiles and determine whether the UACC is appropriate. For those profiles where the UACC is excessive, you will have to determine who really needs access before changing the UACC. To find out who is accessing these data sets, review SMF data to determine who is accessing the data sets with greater than READ access. You can then build PERMIT commands based on the review of the SMF data.</td>
</tr>
</tbody>
</table>
## Assessment Finding #4

<table>
<thead>
<tr>
<th>Finding</th>
<th>RACF Database is not Adequately Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Severe</td>
</tr>
<tr>
<td></td>
<td>The RACF database contains extremely sensitive security information. No access to the RACF database is required for normal administration activities using either RACF commands or the RACF provided ISPF panels. A user who has read access to the RACF database could make a copy and then use a cracker program to find the passwords for user IDs and could obtain a list of user IDs and resources.</td>
</tr>
<tr>
<td>Recommended Best Practice and Remediation</td>
<td>Review the protection for the RACF database and remove any entries granting access higher than NONE, other than the senior RACF administrators and system staff running RACF database utilities.</td>
</tr>
</tbody>
</table>
## Assessment Finding #5

<table>
<thead>
<tr>
<th>Finding</th>
<th>Excessive Access to APF Libraries</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk - Severe</strong></td>
<td><strong>UPDATE</strong> or higher access to an APF library can allow an individual to create an authorized program which can bypass security controls and execute privileged instructions. <strong>Recommended</strong></td>
</tr>
<tr>
<td><strong>Best Practice and Remediation</strong></td>
<td>UPDATE or higher access should be limited to senior systems support staff. Review all accesses to APF libraries and remove or change inappropriate access entries. Ensure that UPDATE and higher accesses are being logged.</td>
</tr>
</tbody>
</table>
## Assessment Finding #6

### Finding

**Risk - Severe**

### Recommended Best Practice and Remediation

<table>
<thead>
<tr>
<th>General Resource Profiles in WARN Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Resource profiles defined in WARN mode specifies that even if access authority is insufficient, RACF is to issue a warning message and allow access to the resource. RACF also records the access attempt in the SMF record. In effect, most all users have full access to any resource that is protected by a profile in WARN mode.</td>
</tr>
<tr>
<td>Monitor the SMF data on a daily basis to determine if the accesses to these resources are due to the WARN mode. The reports will indicate the usage of these resources for users who are not specifically defined to the access list. If the accesses are appropriate, grant the user/group the access required. Remove WARN mode from all general resource profiles once analysis is complete.</td>
</tr>
<tr>
<td>Finding</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>Risk - Severe</td>
</tr>
<tr>
<td>Recommended Best Practice and Remediation</td>
</tr>
<tr>
<td>Finding</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td><strong>Risk - High</strong></td>
</tr>
<tr>
<td><strong>Recommended</strong></td>
</tr>
<tr>
<td><strong>Best Practice and Remediation</strong></td>
</tr>
</tbody>
</table>
## Assessment Finding #9

<table>
<thead>
<tr>
<th>Finding</th>
<th>Improper Use or Lack of UNIXPRIV Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk - High</strong></td>
<td>The UNIXPRIV class resource rules are designed to give a limited subset of the superuser UID (0) capability. When implemented properly, UNIXPRIV profiles can significantly reduce the unnecessary requests for assignment of UID (0) to user IDs.</td>
</tr>
<tr>
<td><strong>Recommended Best Practice and Remediation</strong></td>
<td>Review the users’ activity that are currently defined as SUPERUSERS to determine if more granular profiles may be defined in the UNIXPRIV class that will authorize their activity. Refine the access list and define more granular profiles based upon the superuser functions that the users with UID(0) need.</td>
</tr>
</tbody>
</table>
Assessment Finding #10

<table>
<thead>
<tr>
<th>Finding</th>
<th>Started Task IDs are not Defined as PROTECTED IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk - High</td>
<td>User IDs associated with started tasks should be defined as PROTECTED which will exempt them from revocation due to inactivity or excessive invalid password attempts, as well as being used to sign on to an application.</td>
</tr>
<tr>
<td>Recommended Best Practice and Remediation</td>
<td>Review all started task user IDs that are not protected. Determine if the user IDs are used for any other function that might require a password. Define the started task user IDs as PROTECTED for those tasks that do not require a password.</td>
</tr>
</tbody>
</table>
First step is establishing an IAM framework to properly provision and deprovision access to z/OS resources and enhance the productivity of the organization through Role Based Access models.

Second step is establishing a security operations monitoring framework that effectively monitors the z/OS environment for intrusions and misuse of resources.

Third step is establishing a security policy for z/OS and ensuring the policy is enforced at all times to ensure the integrity of the z/OS platform.

Fourth step is establishing and maintaining a data security warehouse where risk analysis is performed to determine unusual data usage patterns that may be an indication of a security breach or fraud.
It’s All about Risk

• What Risks Do Senior Executives Care About


  – Reputational Risks – loss of prestige, customers, sales.

  – Legal Risks – going to jail, being subject to law suits, or being fined by an industry or government entity.
Managing Your Risks

• What is the likelihood that an event will occur?
  – Attempt to access your system without authorization?

• If an event occurs, will it have an impact?
  – Will they be able to access resource on your system?

• How bad would that impact be?
  – ???

©2015 Vanguard Integrity Professionals, Inc. All Rights Reserved. You have a limited license to view these materials for your organization’s internal purposes. Any unauthorized reproduction, distribution, exhibition or use of these copyrighted materials is expressly prohibited.
Vulnerability Assessment Objectives

- Insure effective security controls implementation
- Verify security configuration settings which could create exposure conditions
- Remediate exposures to improve existing level of security
Vulnerability Assessment Approach

Data Collection
This is the data collection phase to be able to assess the environment.

Data Analysis
This is the data analysis phase where the data collected is analyzed for any potential vulnerabilities.

Report
This is the report phase where the consultant creates a findings report and discusses the findings and recommendations with the customer.

Remediation
This is remediation phase where the Vanguard consultant explains the results of the data analysis and provides remediation advice.
Conclusion

Questions?
Thank You!

For more information, please visit:
http://www.go2vanguard.com
sales@go2vanguard.com

©2015 Vanguard Integrity Professionals, Inc. All Rights Reserved. You have a limited license to view these materials for your organization's internal purposes. Any unauthorized reproduction, distribution, exhibition or use of these copyrighted materials is expressly prohibited.