Performing a z/OS® Vulnerability Assessment

Part 1 - Data Collection

Presented by

Vanguard Integrity Professionals
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, 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. Vanguard Administrator, Vanguard Advisor, Vanguard Analyzer, Vanguard Configuration Manager, Vanguard zSecurity University, and Vanguard Security & Compliance are trademarks of Vanguard Integrity Professionals – Nevada.
1. **Introduction**
   This section introduces this vulnerability assessment webinar series and relationship between the three (3) episodes. It further discuss the reasons for doing regular vulnerability assessments.

2. **Scope and Tooling**
   This section introduces the scope of the vulnerability assessment for z/OS and the Vanguard Tools required to perform the z/OS security data analysis.

3. **Data Collection Examples and Risk Clarifications**
   This section discusses the actual data collection, leveraging the tools discussed in the prior section, and associated risk data related to the findings.
Performing a z/OS Vulnerability Assessment – Data Collection

INTRODUCTION
Webinar Series Overview

**Session 1**

**Data Collection**
- February 27<sup>th</sup> 8am Pacific / 11am Eastern
- March 5<sup>th</sup> 11am Pacific / 2pm Eastern
- March 11<sup>th</sup> Noon Pacific / 3pm Eastern

**Session 2**

**Data Analysis**
- March 20<sup>th</sup> 7am Pacific / 10am Eastern
- March 26<sup>th</sup> 10am Pacific / 1pm Eastern
- April 1<sup>st</sup> 1pm Pacific / 4pm Eastern

**Session 3**

**Remediation**
- April 10<sup>th</sup> 8am Pacific / 11am Eastern
- April 16<sup>th</sup> 11am Pacific / 2pm Eastern
- April 22<sup>nd</sup> Noon Pacific / 3pm Eastern
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 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."
The Situation

- The Mainframe is still an important platform
- Security can fall short
  - Creating high-risk vulnerabilities
- Lack of formal programs

Gartner Research

Publication Date: 20 January 2010

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.
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
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
- Execute all of the above
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.
The identified Security Issues present risk to regulatory / industry compliance standards depending on the data present within the assessed system.
Vanguard’s “Best Practices”

Vanguard 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
Vanguard's Assessment DB & Matrix

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

©2014 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

Improve Security Posture on z/OS
Performing a z/OS Vulnerability Assessment – Data Collection

SCOPE AND TOOLS
Vulnerability Assessment Scope

Scope: Vanguard Top 10 z/OS Risks Identified in Customer Security Assessment

1. Excessive Number of User IDs with No Password Interval
2. Inappropriate Usage of z/OS UNIX® Superuser Privilege UID(0)
3. Started Task IDs are not Defined as PROTECTED IDs
4. Dataset Profiles with UACC Greater than READ
5. Improper Use or Lack of UNIXPRIV Profiles
6. Dataset Profiles with UACC of READ
7. Excessive Access to the SMF Data Sets
8. RACF® Database is not Adequately Protected
9. Excessive Access to APF Libraries
10. Inappropriate Access to FACILITY BPX.DAEMON Profile

Note: Data collected from hundreds of security assessments performed by Vanguard Integrity Professionals.
Vanguard Tools Requirements

Vanguard

Provides Identity & Access Management solutions and Governance, Risk & Compliance solutions for z/OS and other enterprise platforms.

Vanguard Administrator™
Simplify and Enhance Security Management Functions on systems running IBM®'s Security Server™ (RACF)

Vanguard Analyzer™
Delivers expert-level Vulnerability Assessments and Audit results for System z® in minutes

Vanguard Advisor™
Offers the most comprehensive Event Detection, Analysis and Reporting package for the z/OS environment

Vanguard Configuration Manager™
Provides the fastest and most accurate method to verify that mainframe security configuration controls are in compliance with the DISA STIGs

©2014 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 Approach

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

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

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

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

Today’s Webinar

N/A
Performing a z/OS Vulnerability Assessment – Data Collection

DATA COLLECTION
# Assessment Finding #1

**Finding**

Excessive Number of User IDs with No Password Interval

**Report Generation**

Administrator: USER SUMMARY (Fastpath 3;1;1)
Mask: Protected = N, PWD Interval = 0, Revoked = N
Vanguard Configuration Manager: RACF0580

**Risk**

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.
## Assessment Finding #2

<table>
<thead>
<tr>
<th>Finding</th>
<th>Inappropriate Usage of z/OS UNIX Superuser Privilege UID(0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Generation</td>
<td>Administrator: USER OMVS SUMMARY (Fastpath 3;5;9;1)</td>
</tr>
<tr>
<td></td>
<td>Mask: UID = 0</td>
</tr>
<tr>
<td></td>
<td>Vanguard Configuration Manager: ZUSS0046</td>
</tr>
<tr>
<td>Risk</td>
<td>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. Since the UNIX environment is the z/OS portal for critical applications such as file transfers, Web applications, and TCPIP connectivity to the network in general, the ability of these superusers to accidentally or maliciously affect these operations is a serious threat.</td>
</tr>
</tbody>
</table>
## Assessment Finding #3

### Finding

Started Task IDs are not Defined as PROTECTED IDs

### Report Generation

Administrator: USER PROFILE SUMMARY (Fastpath 3;1;1)

Mask: Protected = N and Group = STC Group Name

Vanguard Configuration Manager: RACF0650

### Risk

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.
**Assessment Finding #4**

<table>
<thead>
<tr>
<th>Finding</th>
<th>Dataset Profiles with UACC Greater than READ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Generation</td>
<td>Administrator: DATA SET PROFILE SUMMARY (Fastpath 3;3;1)</td>
</tr>
<tr>
<td></td>
<td>Mask: UACC GT R</td>
</tr>
<tr>
<td>Risk</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>
</tbody>
</table>
Assessment Finding #5

**Finding**

Improper Use or Lack of UNIXPRIV Profiles

**Report Generation**

**Risk**

Administrator: GENERAL RESOURCE ACCESS LIST (Fastpath 3;4;4) Mask: Class = UNIXPRIV

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.
### Assessment Finding #6

<table>
<thead>
<tr>
<th>Finding</th>
<th>Dataset Profiles with UACC of READ</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Report Generation</strong></td>
<td>Administrator: DATA SET PROFILE SUMMARY (Fastpath 3;3;1)</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td>Mask: UACC EQ R</td>
</tr>
<tr>
<td></td>
<td>Data sets that are protected by a RACF profile with a UACC of READ will allow most users with system access to read or copy sensitive and critical data residing in these data sets.</td>
</tr>
</tbody>
</table>
Assessment Finding #7

**Finding**

Excessive Access to the SMF Data Sets

**Report Generation**

Analyzer: SMF Environment Analysis – option 3;H
Enter DSN Command to display SMF Dataset Information
Vanguard Configuration Manager: ACP00180

**Risk**

SMF data collection is the system activity journaling facility of the z/OS system. With the proper parameter designations, it serves as the basis to ensure individual user accountability. The ability to READ SMF data enables someone to identify potential opportunities to breach your security. If UPDATE or higher access is granted, a risk of audit log corruption exists. Access control for the unloaded data is critical to ensure a valid chain of custody.
## Assessment Finding #8

### Finding

RACF Database is not Adequately Protected

### Report Generation

Analyzer: Database Analysis – option 3;3
Enter R next to each data set
Vanguard Configuration Manager: ACP00120

### Risk

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.
## Assessment Finding #9

<table>
<thead>
<tr>
<th>Finding</th>
<th>Excessive Access to APF Libraries</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Report Generation</strong></td>
<td></td>
</tr>
<tr>
<td>Analyzer: Sensitive/Critical Data Sets Analysis Batch – option 4;B</td>
<td></td>
</tr>
<tr>
<td>Enter R next to Authorized Program Facility (APF) Table</td>
<td></td>
</tr>
<tr>
<td>Enter YES for RACF detail</td>
<td></td>
</tr>
<tr>
<td>Vanguard Configuration Manager: ACP00060</td>
<td></td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td></td>
</tr>
<tr>
<td>UPDATE 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.</td>
<td></td>
</tr>
</tbody>
</table>
# Assessment Finding #10

<table>
<thead>
<tr>
<th>Finding</th>
<th>Inappropriate Access to FACILITY Class BPX.DAEMON Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Generation</td>
<td>Administrator: GENERAL RESOURCE ACCESS LIST (Fastpath 3;4;4) Mask: Class=FACILITY and Profile=BPX.DAEMON</td>
</tr>
<tr>
<td>Risk</td>
<td>Daemons are processes that perform services for other users. In order to do this, a daemon must be able to change its identity temporarily to the identity of the user it will perform work for. The RACF FACILITY class profile called BPX.DAEMON can be used to control the use of the daemon functions.</td>
</tr>
</tbody>
</table>

©2014 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.
Performing a z/OS Vulnerability Assessment – Data Collection

WRAP-UP
Webinar Series Overview

**Session 1**
**Data Collection**
- February 27th
  8am Pacific / 11am Eastern
- March 5th
  11am Pacific / 2pm Eastern
- March 11th
  Noon Pacific / 3pm Eastern

**Session 2**
**Data Analysis**
- March 20th
  7am Pacific / 10am Eastern
- March 26th
  10am Pacific / 1pm Eastern
- April 1st
  1pm Pacific / 4pm Eastern

**Session 3**
**Remediation**
- April 10th
  8am Pacific / 11am Eastern
- April 16th
  11am Pacific / 2pm Eastern
- April 22nd
  Noon Pacific / 3pm Eastern

Please join us next time and have your data with you.
To register for a training course or for more information: go2vanguard.com

Customer Savings: Special Discounts for software customers and VSC 2013 attendees

Don’t forget that all of the zSecurity University™ courses are eligible for CPE Credits and all course materials are provided on a tablet computing device that the attendee keeps at the end of the class.
Learn more about Auditing and Assessments at Vanguard Security & Compliance™ 2014

VANGUARD SECURITY & COMPLIANCE 2014

SECURE YOUR ENTERPRISE

June 23-27, 2014 | LAS VEGAS, NV