TUTORIAL: PROTECTING EVERY PATH INTO YOUR SYSTEM WITH RACF

Stuart Henderson
the Henderson Group
Bethesda, MD
(301) 229-7187
www.stuhenderson.com

AGENDA

I. INTRODUCTION

II. JCL PATHS: BATCH AND STCs

III. NETWORK PATHS

IV. SUMMARY AND CALL TO ACTION

I. INTRODUCTION

- When We Read About Embarrassing InfoSec Breaches, We Sometimes Wonder "Why Did They Let That Happen?"

- But How Do We Know That We've Secured Everything We Need To?

- Only By Systematically Reviewing

I. INTRODUCTION

- **Today We'll Address One Aspect of This Systematic Review: Paths Into the System**

- **Without Looking: How Many Paths Into Your z/OS System Can You Name Beyond TSO?**

I. INTRODUCTION

SOME THINGS TO KEEP IN MIND

- Your Security Is Not Complete Unless RACF Controls EVERY Path In

- Also Unless the Administration Is Reliable (Not Addressed Here)

- We Need To Treat Each Path Separately

I. INTRODUCTION

SOME DATASET CONCEPTS APPLIED TO PATHS IN

- **ALWAYS-CALL (Does RACF Always Get Control?)**

- **PROTECTALL (What Do We Do If RACF Has No Matching Rule?)**

II. JCL PATHS: BATCH AND STCs

- **The Internal Reader (TSO SUBMIT Command) is the Part of JES That Processes JCL**

- **We Can Access It by TSO SUBMIT, by a DD card, by XBM (eXecution Batch Monitor), by FTP, by NJE, and by RJE**

II. JCL PATHS: BATCH AND STCs

- **The Internal Reader is Part of JES. It Is the Single Choke Point Through Which All Batch Jobs Pass**

- **JES Always Calls RACF to Process RACF Userids for All Batch Jobs**

- **We Tell JES to Apply PROTECTALL with the BATCHALLRACF Switch**

II. JCL PATHS: BATCH AND STCs

- **BATCHALLRACF is a Switch (Set with SETR) That Tells JES to Fail Any Batch Job Without a Valid RACF Userid**

II. JCL PATHS: BATCH AND STCs

- **Userids Are Inherited By Batch Jobs**
- **Another Way to Say This Is That JES Propagates Userids From Submittors Onto Batch Jobs**
- **SUBMIT a Batch Job Without a USER= and It Inherits Your TSO ID**

II. JCL PATHS: BATCH AND STCs

- **Suppose You Have All TSO Users Controlled by RACF, and All Started Tasks**

- **Then Almost All or All of Your Batch Jobs Will Have Userids (By Propagation From the Submittor If No Other Way)**

II. JCL PATHS: BATCH AND STCs

- **You Can Check the SMF Type 30 Records (Userid Field Not Equal Zeros) to Ensure That All Your Batch Jobs Run With RACF Userids**

- **There is No WARNING Option for BATCHALLRACF**

II. JCL PATHS: BATCH AND STCs

- XBMALLRACF is Similar to BATCHALLRACF, But Used With Joblets in the JES eXecution Batch Monitor

- Most Commercial Shops Don’t Use XBMALLRACF (Ask Your JES Sysprog)

- If You Don’t Use XBM, Should You XBMALLRACF?

II. JCL PATHS: BATCH AND STCs

- **SURROGAT Is a Resource Class Used To Authorize One Userid to Submit Batch Jobs for a Different Userid Without Having to Provide the Password**

- **Why It Should Be Used With Your Job Scheduling Software (Otherwise All Your Production Batch Jobs Inherit the Same Userid and Look the Same to RACF)**

II. JCL PATHS: BATCH AND STCs

- PROPCNTL is a Resource Class in RACF Used to Tell JES What Userids Not to Propagate

- **Why Would You Want To Use It With CICS Region Userids?**

- **Why Might This Be Difficult?**

- **So What To Do?**

II. JCL PATHS: BATCH AND STCs

- **Started Tasks (Also Named Started Procedures, But Abbreviated STC) Have JCL Like Batch Jobs, But They Are Started By the Operator Command START**

II. JCL PATHS: BATCH AND STCs

- **The START Command Can Be Issued at the Console in the Computer Room**

- **Also From Within a Program, Within a Batch Job, Over NJE and RJE**

- **The OPERCMDS Resource Class Can Be Used to Control Who Can START**

II. JCL PATHS: BATCH AND STCs

- **JCL for STCs and for Batch Jobs is Stored in Proclibs**

- **Do You Know the Names of All the Proclibs Where JCL is Stored?**

- **Do You Know Who Can Update Them? Whether Someone Would Notice?**

II. JCL PATHS: BATCH AND STCs

- **Userids Are Always Checked for STCs, Using the STARTED Resource Class and The Assembler Module ICHRIN03**
- **See Them in the DSMON Started Procedures Report**
- **What Is The Effect of an Entry ** ?**

III. NETWORK PATHS

While JES Handles Batch Work, VTAM Handles Net Work

- **SNA (IBM’s System Network Architecture)**
- **TCP/IP (Transmission Control Protocol / Internet Protocol) and Other IP Protocols**

III. NETWORK PATHS

SNA (IBM’s System Network Architecture)

SNA Is Not Dead. You Use It to Log Onto TSO, CICS, etc. The SNA Messages Are Tunneled Inside TCP, But It’s Still SNA

SNA Is Not Dead. You Use It With Enterprise Extender (Cross Network Binds) Tunneled In UDP

III. NETWORK PATHS

SNA Concept: An APPLID (Application Identifier) is the VTAM Name for a Program with a Signon Screen

Each APPLID is a Path Into Your System

III. NETWORK PATHS

Which APPLIDs Have ALWAYS-CALL for Signons?

Which PROTECTALL?

What of TSO, CICS, DB2, OMEGAMON?

What of the APPLIDS Someone Installed and Never Told You About?

III. NETWORK PATHS

- **TSO and SYS1.UADS, the TSO Segment in RACF, the APPL Resource Class**

- **Which APPLIDs Wised Up After Not Originally Being ALWAYS-CALL?**

- **DB2 and TCPALVER**

- **How to Learn All the APPLIDs**

III. NETWORK PATHS

- **With Enterprise Extender, SNA is Tunneled Inside UDP Packets. You Might Use This to Connect Your SNA Network to a Business Partner’s (Bank to CredCard Processor, for Example)**

III. NETWORK PATHS

- **When VTAM Allowed Cross Network Connections Like Enterprise Extender, It Had to Loosen Some of Its Requirements**
- **(Like the One Preventing Any Connection to a Terminal or APPLID Not Pre-Defined to VTAM)**

III. NETWORK PATHS

- This Makes Cross Network SNA Connections Susceptible to Some of the Same Attacks That Affect TCP/IP (Man in the Middle, Spoofing, DOS)

- Who Is Responsible for Securing These Connections: VTAM Sysprog or RACF Admin or Someone Else?

III. NETWORK PATHS

A Variety of Tools Are Available to Tighten the Security Over Cross Network Connections:

- **Options in the VTAM Configuration File**
- **RACF Resource Classes (VTAMAPPL, APPCLU)**
- **Software Such as the SNA Firewall from Net’Q.**

III. NETWORK PATHS

The IP in TCP/IP Provides Routing, Getting the Message to the Computer It Needs to Reach

TCP Rides On Top of IP, Providing the Application Support Once the Message Reaches the Right Computer

Each Application is Assigned a Port Number to Identify It

III. NETWORK PATHS

Each Port is a Path Into Your System Which You Need to Control

You Can Block the Ports in the TCP/IP Control File: Use Keywords RESTRICTLOWPORTS, DENY, RESERVED, and SAF

III. NETWORK PATHS

Some Applications Can Make It Possible for People to Use Your Computer Without a RACF ID:

- **FTP with Anonymous Login**
- **http with BPX.SERVER, BPX.DAEMON, SURROGAT**
- **rlogin, rexec, rsh (see the .rhosts file)**

Sometimes You Want to Allow This (Customers Reading Your Ads)

III. NETWORK PATHS

Besides TCP, Other Protocols Ride On Top of IP:

- **ICMP**

- **UDP**

How to Manage Them

III. NETWORK PATHS

Who Is Responsible for Securing Each of These?

Is the Quality Assurance and Change Control As Good As What You Have for Production Batch Jobs?

IV. Summary and Call to Action

To Be Able to Demonstrate the Quality of Our Security, We Need to Address Every Path Systematically, Applying:

1. **The ALWAYS-CALL Concept**
2. **The PROTECTALL Concept**
3. **Quality of Administration (Passwords, Naming Standards, Responsibility and Authority, Focused Control of Open Paths)**

IV. Summary and Call to Action

- **If We Don’t Stop to Consider, It’s Easy to Think We’re Protecting Everything Properly, and Still Be Missing Important Coverage.**

IV. Summary and Call to Action

Path In	Always-Call?	Protect all?	Other Controls	Comments
Batch				
XBM				
STCs				
TSO				
CICS				
DB2				
Other SNA				
ftp				
rlogin				
telnet				
httpd				
…				

IV. Summary and Call to Action

Life Is Easier When Protection Is:

- **Automatic**
- **Comprehensive**
- **Simple Enough to Explain on a Cocktail Napkin**

IV. Summary and Call to Action

Thanks for Your Kind Attention