Securing TCP/IP Today Before You're Sorry Tomorrow

Joel Tilton
RACF Engineer
Mainframe Evangelist
May 2019

About Joel Tilton, CISSP

- Joel Tilton is a former employee of IBM, where he got his start with mainframes, who continues to champion mainframe security issues and solutions.
- Over 20+ years technical IT experience, the majority of which was gained in hands-on technical roles, performing a variety of duties in diverse and complex environments.
- The majority of Joel's experience is focused on IBM mainframe systems, where he performs as a Technician and Project Manager. Joel's specialist subject is IT Security, in particular z/OS and associated subsystems (CICS, DB2, MQ, zSecure, etc.) security with RACF.
- Joel is also an active member of the Tampa Bay RUG (RACF User Group) which meets jointly with the NY RUG. Joel has a true passion for security and the mainframe. Long live the mainframe!
- https://www.linkedin.com/in/joeltilton
- RACFEngineer@gmail.com
- 702-483-RACF (Google Voice) ← Because it's cool!

Disclaimers

- All products, trademarks, and information mentioned are the property of the respective vendors.
- Mention of a product does not imply a recommendation.
- Always test new profiles on a non-production system.
- Only you can prevent IPLs…
- The views expressed are his own personal views, and are not endorsed or supported by, and do not necessarily express or reflect, the views, positions or strategies of his employer

SERVAUTH – Lots of Fancy Stuff

- z/OS Communications Server e.g. TCPIP calling SAF has come a long way
- We can secure
  - Ports ← Start here
  - IP Sockets
  - NETSTAT commands ← One RACF Profile
    - EZB.NETSTAT.**
  - Virtual IP Addresses
  - And much much more….
  - https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.halz002/security_tcpip_resrcs.htm

Why?

- Before I implement new security – why?
- Much better control of who is accessing your mainframe over TCP/IP
- Do you really trust the firewall rules?
- Control ports to prevent data bleed outside the company
- Control who can view TCP/IP live
  - Config, NETSTAT
- So why haven't you started?

What is a Port?

- An IP address is used to route the message to your computer. Once it arrives there, TCP uses the port number to know which program like ftp or email to hand it to
- From a SERVAUTH perspective…
  - Any mainframe program binding to
  - and/or listening on a TCPIP Port
  - SYS1.TCPIP.PROFILE

- Why?
  - Ensure ports can not be abused
  - Software can only bind and listen on assigned ports

Why Port Security with RACF?

NATIVE TCP/IP

- Reservation by Jobname
- Can be spoofed
  - Unless JESJOBS profiles protecting jobnames
- Violations not well logged
- Unreserved ports not easily controlled
- Low Ports possibly protected with
- RESTRICTLOWPORTS
  - PORT JOBNAME reservation takes precedence
  - Did I mention JESJOBS?!

RACF

- Reservation by SAFNAME
- Cannot be spoofed
  - RACF profile FINAL answer
- Successes or Violations logged to SMF (type 80)
- Unreserved ports easily controlled
- Low Ports ALWAYS protected with RESTRICTLOWPORTS
  - EZB.PORTACCESS profiles take precedence

RESTRICTLOWPORTS & UID(0)

PORT AUTHORITY

- UID(**0**)
- BPX.SUPERUSER
- SAF

RESTRICTLOWPORTS

- Access Granted
- Access DENIED, even after SU
- RACF in total Control
  - Even For Low Ports, 0 – 1023

EZB.PORTACCESS Profile Syntax

EZB.PORTACCESS.*sysname*.*tcpname*.*safname*

Qualifier	Description	Recommendation
sysname	Local SMF ID	• Use * unless per LPAR uniqueness
tcpname	TCPIP started task jobname	• Use * unless multiple stacks • Hopefully Not
safname	Esoteric name coded in port reservation	• Can be generic • 1 – 8 characters • First Position Never **0** (zero) • RFE 75935

RFE 75935
https://www.ibm.com/developerworks/rfe/execute?use_case=viewRfe&CR_ID=75935
Applies to NETACCESS, PORT, PORTRANGE, VIPADYNAMIC & VIPARANGE

SAFNAME Design

- Use known protocol name as SAFNAME
  - HTTP, HTTPS, LDAP, SMTP
  - Plus TCP or UDP to indicate port type
  - HTTPTCP, HTTPSTCP, LDAPTCP, SMTPTCP, SMTPUDP
    - Type 80 logstring does not indicate Protocol ➔ RFE 68402
    - https://www.ibm.com/developerworks/rfe/execute?use_case=viewRfe&CR_ID=68402
- Use generics in profile, as appropriate
  - HTTP*, LDAP*
  - … if appropriate
- Relationship
  - One to MANY port reservations to ONE RACF profile

Sample Port & Portrange Syntax

```
PORT
   20 TCP * NOAUTOLOG SAF FTPDATA   ; FTP SERVER DATA PORT
   21 TCP *           SAF FTP       ; FTP Control Port
   22 TCP *           SAF SSHD      ; SSH SERVER
   23 TCP *           SAF TN3270    ; TN3270
   25 UDP *           SAF SMTP      ; SMTP SERVER
  161 UDP *           SAF SNMP      ; OSNMPD
  162 UDP *           SAF SNMP      ; SNMPQE
  520 UDP *           SAF OMPROUTE  ; OMPROUTE
…
UNRSV TCP *           SAF UNRSVTCP WHENBIND
UNRSV UDP *           SAF UNRSVUDP
;
; ------------------------------------------------------
 PORTRANGE
  1850   101 TCP *        SAF OMEGAMON
  1850   101 UDP *        SAF OMEGAMON
  19000  101 TCP *        SAF OMEGAMON
  19000  101 UDP *        SAF OMEGAMON
```

Example: TN3270 – Reservation

```
PORT 23   TCP TN3270
```

- Non-SAF uses jobname
- Without JESJOBS, submitting a jobname of TN3270 would allow any program to bind to port 23 and use it

```
PORT 23   TCP *          SAF TN3270
```

- With SAF
  - Jobname no longer required

Example: TN3270 – RACF Profile

`EZB.PORTACCESS.*.*.TN3270`

- UACC always NONE
- Permit TN3270 STC user ID with READ
- AUDIT ALL(READ)
  - Audit all port access attempts; failures and successes
  - Including FTP data port; not *that* much more SMF
- WARNING or UACC(READ)
  - Use wisely as an implementation strategy
  - Anything can bind to or listen

NETSTAT PortList

- NETSTAT PORTList tells you what is the SAFNAME as of "NOW"
  - RDEF SERVAUTH EZB.NETSTAT.** UACC(NONE)

```
EZZ2795I Port# Prot User     Flags    Range       IP Address      SAF Name
EZZ2796I ----- ---- ----     -----    -----       ----------      --------
EZZ2797I UNRSV TCP  *        FI                                   UNRSVTCP
EZZ2797I 7     TCP  *        DAF                                  MISCSRV
EZZ2797I 9     TCP  *        DAF                                  MISCSRV
EZZ2797I 19    TCP  *        DAF                                  MISCSRV
EZZ2797I 20    TCP  *        DF                                   FTPDATA
EZZ2797I 21    TCP  *        DAF                                  FTPDN
EZZ2797I 22    TCP  *        DAF                                  SSHD
EZZ2797I 25    TCP  *        DAF                                  SMTP
```

Implementation Strategies

USE WARNING / UACC READ

- Use WARNING mode
- Or UACC(READ)
- Mine Type 80 records

- Con:
  - Anything can bind any program to ports
- Pro:
  - Captures all port access over time

PARSE NETSTAT COMMANDS

- Write a REXX parsing NETSTAT CONN & PORTList output

- Cons:
  - Will not see all port usage
  - Snapshot in time
- Pro:
  - No port exposure assuming JESJOBS active

Planning – Gather Information

- Evaluate running STCs and their ports
  - NETSTAT CONN ➔ What is Listening
  - NETSTAT PORTLIST ➔ How it is Reserved
    - **REMINDER**: SERVAUTH EZB.NETSTAT.** ➔ Attack Vector
  - REXX EXEC compare reservations vs. usage
- Create Spreadsheet of Port Listeners & SAF*names*
- Partner with Network/VTAM Engineer
  - TCPIP profile changes
  - Weekend IPLs
- Update Software Parms
- Implement one system at a time
  - development, test and then production
- REMEMBER: Only **YOU** can prevent IPLs!

SERVAUTH Class Activation

- Activate SERVAUTH Class
  - Quick Survey: SERVAUTH not active?
  - IBM Class Descriptor Table (CDT)
  - **`SETR classact(SERVAUTH) audit(SERVAUTH) raclist(SERVAUTH) generic(SERVAUTH) gencmd(SERVAUTH)`**
    - RC of 4 class but be mindful of SYS1.TCPIP.PROFILE
      - SERVAUTH profiles for DVIPA (Dynamic Virtual IP Address)
      - **`EZD1313I -REQUIRED SAF SERVAUTH PROFILE NOT FOUND `*`RACF profile name`***

Setup RACGLIST Support

- How many have heard of RACGLIST?
- **`RDEFINE RACGLIST SERVAUTH OWNER()`**
  - IPL will **not** refresh in-storage RACF profiles
  - Ensure Sysplex Consistency for RACF
  - By Product…Performance Improvement
  - **`SETR classact(RACGLIST)`**
    `audit(RACGLIST)`
  - **`SETR RACLIST(…) REFRESH`**
    - ➔Builds RACGLIST profiles
  - Recommend for **all** active classes that have profiles

Auditing Port Access

- RACF – Final Port Authority
- **ALL** Port Usage Logged → Type 80
  - Binders and listeners
  - Authorized and unauthorized Use
  - Can other platforms do that?
- LOGSTRING contains port number
  - TCP / UDP Not Recorded! ☹
  - RFE
    - https://www.ibm.com/developerworks/rfe/execute?use_case=viewRfe&CR_ID=68402

Summary

- The journey of 1,000 miles begins with a single step
- Securing TCP/IP using SERAVUTH profiles provides a great defense against TCP/IP attack vectors
- If there's one thing you do:
  - RDEF SERVAUTH EZB.NETSTAT.** UACC(NONE)
- If there's two things you do:
  - Start securing your ports one at a time!

Questions?

Additional Resources

- Techdocs Library – Using SERVAUTH to Protect TCP Port Usage
  - http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100673
- Techdocs – Undesired PortAccess Violations
  - http://www-01.ibm.com/support/docview.wss?rs=852&uid=swg21237916
- Port Access Control Chapter
  - z/OS Communications Server: IP Configuration Guide
  - http://www-01.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.halzoo2/security_tcpip_resrcs_ports.htm
- SERVAUTH Class profiles used by TCP/IP
  - EZB.PORTACCESS syntax
  - http://www-01.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.halzoo2/security_tcpip_resrcs_saf.htm

Even more Useful Resources

- IBM z/OS V2R2 Communications Server TCP/IP Implementation: Volume 4 Security and Policy-Based Networking
  - http://www.redbooks.ibm.com/abstracts/sg248363.html?Open
- RESTRICTLOWPORTS parameter
  - https://www-01.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.halz002/security_tcpip_resrcs_unresvd_ports_low.htm
- TCPIP PROFILE Port Assignments
  - http://www-01.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.halz001/profiletcpipportassignments.htm