

Top 11 Things You Should Be Doing to Secure Your z/OS System - 2018 Edition

Session 22295

Wednesday, March 14, 2018 4:30 PM

Thomas Conley

Pinnacle Consulting Group, Inc. (PCG)

59 Applewood Drive

Rochester, NY 14612-3501

P: (585)720-0012

F: (585)723-3713

pincons@rochester.rr.com



Abstract

Do you need to better secure your z/OS system? Do you have an audit coming up? Do you need to know what to secure? If you answered YES to any of these questions, then this session is for you! The speaker will share over 30 year's experience working in and hardening security for RACF and ACF2 environments. Some of the items on the top 11 list will surprise you!



Agenda

- z/OS Under Attack
- Why is z/OS Under Attack?
- Fight Back Before You Get Hacked
- Choose Your Weapons
- Top 11 List Overview
- Top 11 List Items
- Finally



z/OS Under Attack

- Mainframes are more under attack than ever
- Mainframe vulnerabilities make it easier to crack than most people (i.e. “the common wisdom”) think
- Still think a mainframe can’t be hacked?
- Read these presentations from Philip Young (aka Soldier of Fortran, <https://mainframed767.tumblr.com/>)
 - [How Hackers Breached a Government \(and a Bank\)](#)
 - [Post Exploitation Enumeration Mainframe Hacking - Security Opener](#)
- Mainframe hacking is alive and well
- Mainframe security administrators must come to grips with the fact that their mainframe is vulnerable and a target for attack



Why is z/OS Under Attack?

- It took hackers a while, but they've finally concluded, like Willie Sutton, that mainframes are where the money is
- Windows or Unix POS terminal just front-end to mainframe
- Largest institutions use mainframes to hold and protect critical data
 - Credit Cards
 - Banking
 - Insurance
 - Health-care
 - Government
 - Etc.
- "Western civilization runs on the mainframe" - Tom Rosamilia, IBM



Fight Back Before You Get Hacked

- Tighten down your system now!
- Start with this session and use other resources provided here
- Implement process to continuously monitor and tighten security
- Hardening z/OS not just "one-time" task, it's an "all-the-time" task



Choose Your Weapons

- First and foremost, document EVERYTHING with valid business reasons for why you're doing it
- You need to justify your security settings
 - Privileged users (SPECIAL, NON-CNCL, UID(0), etc.)
 - Critical datasets (LINKLIB, PARMLIB, LPA, APF, etc.)
 - Security exits, policies and procedures, etc.
- Company security organization should SIGN OFF on documentation
- I've seen many sites with inadequate security documentation, resulting in audit findings
- Documenting business reasons for security key to successful audits



Choose Your Weapons

- Internal/external audits
 - Sarbanes-Oxley (SOX)
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Gramm-Leach-Bliley Act (GLBA)
 - Payment Card Industry Data Security Standard (PCI/DSS)
- EU General Data Protection Regulation (GDPR)
 - Newest security regulation, but most far-reaching consequences
 - Significant fines for non-compliance
 - Visit <https://www.eugdpr.org/> for more information
- Use audit results to address deficiencies (hopefully you're proactive and the audits have fewer findings)



Choose Your Weapons

- Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs)
 - DISA provides IT services to support US troops
 - There are STIGs for CA-ACF2, RACF, and CA-TopSecret:
<http://iase.disa.mil/stigs/os/mainframe/Pages/zos.aspx>
 - Frequently updated for currency
 - CA-ACF2, RACF, and CA-TopSecret were last updated 01/26/2018
 - There are jobs to analyze your system
 - They cover z/OS and many other program products running on z/OS
 - STIGs are FREE - your US tax dollars at work!

Choose Your Weapons

- Reporting Tools
 - CA-ACF2 and CA-TopSecret reporting
 - Security add-on products from companies such as IBM, CA, Vanguard, Eberhard Klemens, etc.
- My sessions on RACF Reporting and Auditing
 - [RACF Power Tools - IRRICE, Rexx, IRRADU00, IRRDBU00, Part 1](#)
 - [RACF Power Tools - IRRICE, Rexx, IRRADU00, IRRDBU00, Part 2](#)
 - Sysprog, Audit Thyself!



Sysprog, Audit
Thyself!



Choose Your Weapons

- z/OS Health Checker
 - RACF, CA-ACF2, and CA-TopSecret all have Health Checks to ensure they are operating correctly and that easy holes are closed
 - Health Checks displayed by tools such as SDSF, (E)JES, IOF, SYSVIEW, etc.
- Two security consultant websites with excellent information:
 - Robert Hansel's [RSH Consulting](#)
 - Stu Henderson's [The Henderson Group](#)



Choose Your Weapons

- Google following for their SHARE, IBM zTechU, DefCon, etc. presentations:
 - Philip Young
 - Julie Bergh, Mark Nelson, Bruce Wells - IBM
 - Ray Overby - Key Resources
 - Chad Rikansrud, Mark Wilson - RSM Partners
 - Brian Marshall - Vanguard



Top 11 List Overview

- I developed this Top 11 List based upon what I've seen at my clients
- While far from scientific, my Top 11 List agrees with many items on other security industry lists
- Top 11 List leans towards RACF, but I've tried to cover CA-ACF2 and CA-TopSecret also
- Top 11 List items apply equally to all ESM's
- YMMV, but many if not all Top 11 items likely to apply to you
- For RACF, ICETOOL reports will be indicated where applicable



#11 - WARNING Mode Profiles

- WARNING mode profiles useful to define new access without creating production issues
- Problem is WARNING mode often left on
- Remediate WARNING mode by reviewing accesses allowed and add appropriate accesses
- RACF ICETOOL reports
 - WARN - Accesses allowed due to WARNING mode profile
 - WNDS - Data set profiles in WARNING mode
 - WNGR - General resource profiles in WARNING mode



#10 - Obsolete User Removal

- Do you have documented procedure for removing obsolete users (fired, resigned, contractors, etc.)?
- Especially important if obsolete user has high privilege or authority
- Run RACF IRRRID00 utility periodically (e.g. every 30 days) to remove obsolete access list entries
- Necessary because RACF does not scan access lists when user is deleted



#10 - Obsolete User Removal

- Terminated employees should have userid deleted everywhere ASAP
- Process to delete terminated employees should be fully-documented
 - Backup and delete/rename user datasets
 - Delete user catalog alias
 - Delete user from RACF and run IRRRID00 immediately
 - Delete user from HMC
 - Delete user Email account(s), Active Directory, Unix Accounts, etc.
- RACF ICETOOL report
 - URVK - User IDs which are currently revoked



#9 - Obsolete Profile/Rule Removal

- Obsolete profiles and rules are more difficult to clean up
- Profile or rule may be used infrequently (e.g. once a year)
- Easiest profiles/rules to clean up are for old program products, usually identified by VxRyMz type qualifiers in dataset name
- CA-Cleanup software tracks profile/rule use for RACF, CA-ACF2, and CA-TopSecret
- IBM zSecure Access Monitor performs similar checks for RACF

#8 - TSO User Brute Force Enumeration

- Due to TSO LOGON panel error messages, it is possible to enumerate valid TSO userids on z/OS

```
IKJ56420I Userid JUNK not authorized to use TSO
IKJ56714A Enter current password for IBMUSER
IKJ56421I PASSWORD NOT AUTHORIZED FOR USERID
IKJ56429A REENTER -
```

- IKJ56420I indicates invalid userid
- IKJ56714A indicates valid userid
- IKJ56421I/IKJ56429A indicates invalid password
- No limit, can be done over and over again once TN3270 session established
- Hackers love this, it's all they need to determine every TSO userid!

#8 - TSO User Brute Force Enumeration

```
zPDT
File Edit Font Transfer Macro Options Window Help

----- TSO/E LOGON -----
IKJ56420I Userid JUNK not authorized to use TSO

Enter LOGON parameters below:

*Userid    ==> JUNK
Password   ==>
Procedure  ==>
Acct Nmbr  ==>
Size       ==>
Perform    ==>
Command    ==>

Enter an 'S' before each option desired below:
        -Nomail          -Nonotice          -Reconnect          -OIDcard

PF1/PF13 ==> Help      PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field

MBA 0.0 a 6,20
```

#8 - TSO User Brute Force Enumeration

```
zPDT
File Edit Font Transfer Macro Options Window Help

----- TSO/E LOGON -----
IKJ56421I PASSWORD NOT AUTHORIZED FOR USERID
IKJ56429A REENTER -
Enter LOGON parameters below:
Userid    ==> IBMUSER
Password  ==> 
Procedure ==> ISPFPROC
Acct Nmbr ==> ACCT#
Size      ==> 2096128
Perform   ==>
Command   ==> ISPF

RACF LOGON parameters:
New Password ==>
Group Ident  ==>

Enter an 'S' before each option desired below:
-Nomail      -Nonotice    S -Reconnect    -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field

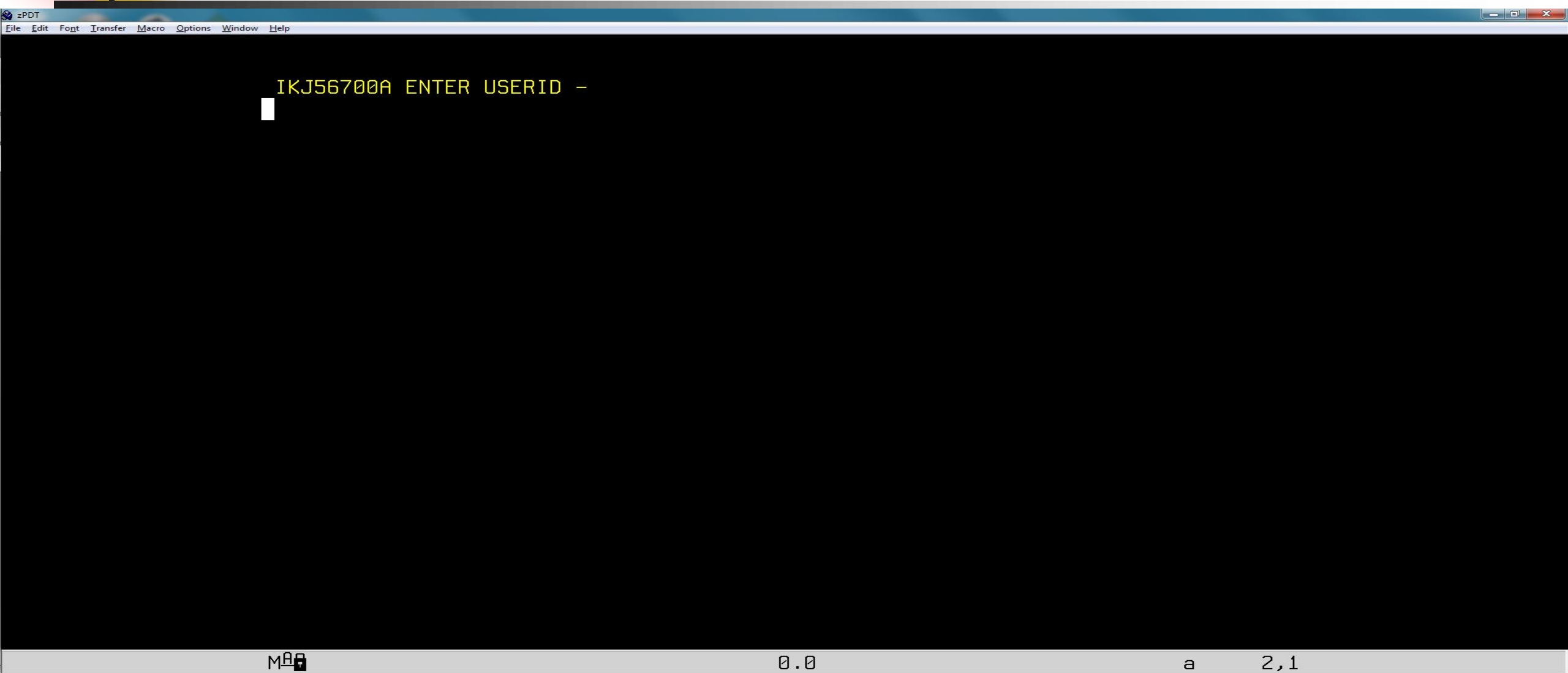
MBA 0.0 a 8,20
```

#8 - TSO User Brute Force Enumeration

- TSO APAR OA44855 addresses this serious integrity exposure
- Enable IKJTSOxx option:
LOGON PASSWORDPREPROMPT (ON)
- TSO LOGON panel does not display data until valid userid/password provided
 - No "PASSWORD NOT AUTHORIZED"
 - No "Userid xxxxxxxx not authorized to use TSO"
- Error message obfuscates reason for failed logon

IKJ56474I USERID OR PASSWORD IS INCORRECT OR NOT AUTHORIZED

#8 - TSO User Brute Force Enumeration



The image shows a terminal window titled 'zPDT' with a menu bar containing 'File', 'Edit', 'Font', 'Transfer', 'Macro', 'Options', 'Window', and 'Help'. The terminal content displays the text 'IKJ56700A ENTER USERID -' followed by a white cursor block. At the bottom of the terminal window, there is a status bar with the text 'MBA 0.0 a 2,1'.

#8 - TSO User Brute Force Enumeration

```
zPDT
File Edit Font Transfer Macro Options Window Help

IKJ56700A ENTER USERID -
guesusr
IKJ56476I ENTER PASSWORD

IKJ56474I USERID OR PASSWORD IS INCORRECT OR NOT AUTHORIZED
*****
█

MMA X SYSTEM          0.0          a      7,1
```

#8 - TSO User Brute Force Enumeration

```
zPDT
File Edit Font Transfer Macro Options Window Help

----- TSO/E LOGON -----

Enter LOGON parameters below:          RACF LOGON parameters:

Userid    ==> IBMUSER

Procedure ==> I SPFPROC                New Password ==>

Acct Nmbr ==> ACCT#                    Group Ident  ==>

Size      ==> 2096128

Perform   ==>

Command   ==> ISPF

Enter an 'S' before each option desired below:
      -Nomail          -Nonotice      S -Reconnect          -OIDcard

PF1/PF13 ==> Help      PF3/PF15 ==> Logoff      PA1 ==> Attention      PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field

MBA 0.0 a 10,20
```




#8 - TSO User Brute Force Enumeration

- Inhibitors to implementing LOGON PASSWORDPREPROMPT(ON)
 - Screen-scraping apps
 - VTAM session manager macros
 - HLLAPI apps
 - TSO logon exits
- Know your TSO LOGON environment
- Consider also enabling client certs for your TN3270 application
 - Challenge to deploy and administer
 - Effective way to thwart external hacker from using TN3270 to attack internet-facing mainframe
 - Prevents other enumeration attacks via VTAM and CICS



#7 - Unsecure Certs and Ciphers

- Cryptography is extremely dynamic field
- Yesterday's secure cert/cipher is today's crackable exploit
- Choose certs/ciphers with highest level of security
- Software maintenance or upgrades typically required to support current secure ciphers (also referred to as cipher suites)
 - BlueZone V5.2 to V7.1 upgrade required to support AES256 SHA384
 - OpenSSL upgrade required to support SHA384



#7 - Unsecure Certs and Ciphers

- Don't use SHA1 hashing, it's proven to have collisions
- NSA no longer recommends SHA256 or AES128
- I recommend AES256 SHA384 as MINIMUM level for TLSv1.2
 - You may need to upgrade your TN3270 clients
 - We upgraded BlueZone V5.2 to V7.1 to handle AES256 SHA384
- RSA1024 was deprecated in 2011
 - Why 1024-bit RSA keys are not strong enough
 - Many sites still use RSA1024 certs
 - You should upgrade your RS1024 certs to RSA2048 ASAP
 - Install RSA2048 certs for RECEIVE ORDER and ShopZ



#7 - Unsecure Certs and Ciphers

- Other unsecure ciphers (if you see these in the cipher name, run)
 - NULL (no encryption)
 - Anything starting with SSL_
 - DES (includes 3DES)
 - SHA (implies SHA-1)
 - RC4
 - MD5
 - AES_128
 - SHA256
- Please don't refer to unsecure certs/ciphers as "insecure"



#6 - Secure Your Internal Network

- One of the first things I check for new client
- Is AT-TLS enabled? ("YES" is the correct answer)
- Is SSL/TLS enabled? (If "YES", get to AT-TLS as soon as possible)
 - SSLv3/TLSv1.0 no longer considered secure
- Is OpenSSH in use? ("YES" is the correct answer)
- "NO" is frequent answer for above questions
- Many sites think internal network is secure
- Nothing could be further from the truth
- Wireshark is a Windows "sniffer" for Ethernet
 - Very easy to install and use, can easily detect TSO passwords in the clear
 - [Wireshark Hands-On Lab](#)



#6 - Secure Your Internal Network

- OpenSSH replaces rlogin, rcp, and ftp with secure alternatives
- z/OS supports OpenSSH in Ported Tools
- [IBM Ported Tools Open SSH - Quick Install Guide](#)
- [Configuring OpenSSH on z/OS Hands-on Lab](#)
- But I've got a VPN!
- VPN encrypts your tunnel over the Internet, but once you're on your internal network, is the traffic still encrypted?



#6 - Secure Your Internal Network

- PCI mandates AT-TLSv1.1 (minimum), by June 30, 2018
- AT-TLS installation looks daunting, so...
- I attended lots of AT-TLS sessions at SHARE, zTechU, etc., and read every manual I could about AT-TLS
 - Not one had a step-by-step method
 - Not one had this Redbook, which I discovered at SHARE in Providence:
[IBM z/OS V2R2 Communications Server TCP/IP Implementation: Volume 4 Security and Policy-Based Networking](#)
 - Redbook has been around since at least V1R12!
 - Redbook eventually shows steps I'll cover more quickly
 - The Redbook is an excellent reference
 - Wish I'd known about it when I started implementing AT-TLS



#6 - Secure Your Internal Network

- In hindsight, TLS implementation fairly straightforward
 - TCPIP PROFILE changes
 - TN3270 config changes
 - Generate certificate
 - Create AT-TLS policy (manually or z/OSMF Config Assistant)
 - Enable PAGENT (Policy AGENT) started task
 - Create SERVAUTH security profiles
- Use following examples to implement AT-TLS in 3-4 hours
- I take the arrows, you get the glory!

#6 - Secure Your Internal Network

- TCPIP required profile changes for AT-TLS
- Add TTLS parm to TCPIPCONFIG
TCPCONFIG RESTRICTLOWPORTS TTLS
- For one TCP/IP stack, AUTOLOG PAGENT to so it starts with TCPIP
AUTOLOG
PAGENT ; Policy Agent
- For multiple TCP/IP stacks, add PAGENT to automation or
COMMNDxx instead of AUTOLOG
- Add DELAYSTART TTLS to AUTOLOG tasks requiring TTLS
PORTMAP DELAYSTART TTLS ; Portmap Server
LPSERVE DELAYSTART TTLS ; LPD Server

#6 - Secure Your Internal Network

- TN3270 configuration changes less extensive than TCPIP
- Use TTLSport statement in TelnetParms

```
TelnetParms                ; AT-TLS TN3270E Telnet server port
    TTLSport 992
; Conntype secure
; ClientAuth None
; SSLtimeout 10
EndTelnetParms
```

- Comment out or delete other options
- All other options specified in AT-TLS PAGENT policy

#6 - Secure Your Internal Network

- Existing SSL Certificate may suffice
- RACF commands to generate self-signed certificates ("borrowed" from Tim Raley's TLS session, available [here](#)):

```
racdcert gencert certauth -
  subjectsdn(cn('TN3720 Certificate Authority (CA)') -
  o('Pinnacle Consulting Group, Inc.') -
  ou('TN3270 Cert Org Unit') c('US')) -
  RSA size(2048) -
  notbefore(date(2015-09-11)) -
  notafter(date(2050-09-11)) -
  keyusage(certsign) -
  withlabel('TN3270 CA')
racdcert gencert site -
  subjectsdn(cn('TN3270 Site Certificate') -
  o('Pinnacle Consulting Group, Inc.') -
  ou('TN3270 Site Org Unit') c('US')) -
  RSA size(2048) -
  notbefore(date(2015-09-11)) -
  notafter(date(2050-09-11)) -
  withlabel('TN3270 SharedSite1') -
  signwith(certauth label('TN3270 CA'))
setropts raclist(digtring) refresh
setropts raclist(digtcert) refresh
```



#6 - Secure Your Internal Network

- Self-signed cert still vulnerable to "man-in-the-middle" attack so use real cert if you have one
- No substitute for real cert, but passwords are at least encrypted until you implement a strong certificate

#6 - Secure Your Internal Network

- Create keyring and connect certificates and users

```
racdcert id(START1) addring(TCPIPRing1)
racdcert id(START1) connect(CERTAUTH -
  label('TN3270 CA') ring(TCPIPRing1) -
  usage(certauth) )
racdcert id(START1) connect(SITE -
  label('TN3270 SharedSite1') ring(TCPIPRing1) -
  default usage(personal) )
setropts raclist(digtring) refresh
setropts raclist(digtcert) refresh
rl facility IRR.DIGTCERT.LISTRING all
PE IRR.DIGTCERT.LISTRING CL(FACILITY) -
  ID(START1) ACCESS(read)
SETROPTS RACLIST(FACILITY) REFRESH
rl facility IRR.DIGTCERT.LISTRING all
RL FACILITY IRR.DIGTCERT.GENCERT ALL
RDEF FACILITY IRR.DIGTCERT.GENCERT UACC(NONE) -
  OWNER(SYS1)
PE IRR.DIGTCERT.GENCERT CL(FACILITY) -
  ID(START1) ACCESS(CONTROL)
SETROPTS RACLIST(FACILITY) REFRESH
RL FACILITY IRR.DIGTCERT.GENCERT ALL
```



#6 - Secure Your Internal Network

- I used z/OSMF Configuration Assistant to create PAGENT policy
- Really unnecessary for AT-TLS, generated policy is cookie cutter
- z/OSMF Configuration Assistant should be used if you enable other PAGENT features such as Intrusion Detection, QOS, etc.
- By default, you'll need two USS files:
 - /etc/pagent.conf
 - /etc/pagent_TTLS.conf
- IBM provides samples for both files
 - /usr/lpp/tcpip/samples/pagent.conf
 - /usr/lpp/tcpip/samples/pagent_TTLS.conf
- Updating samples easier than Config Assistant for one TCPIP stack

#6 - Secure Your Internal Network

- /usr/lpp/tcpip/samples/pagent.conf is nearly all comments
- You only really need two lines (remove all QoS statements):

```
CommonTTLSSConfig /etc/pagent_TTLS.conf
```

```
TTLSSConfig /etc/pagent_TTLS.conf FLUSH PURGE
```

- FLUSH PURGE deletes TTLS rules if PAGENT comes down
- /usr/lpp/tcpip/samples/pagent_TTLS.conf sample contains FTP, Rexec, etc.
- Following is pagent_TTLS.conf for TN3270 only:



#6 - Secure Your Internal Network

```
##
## AT-TLS Policy Agent Configuration file for:
##   Image: SYSA
##   Stack: TCPIP
##
## Created by the IBM Configuration Assistant for z/OS Communications Server
## Version 2 Release 2
## Backing Store = Conley
## Install History:
## 2017-03-28 18:12:04 : Save To Disk
## 2017-03-28 17:28:43 : Save To Disk
##
## TLS default rules: Default_TN3270-Server|
## End TLS default rules
##
## End of Configuration Assistant information
```


#6 - Secure Your Internal Network

```
TTLRule Default_TN3270-Server~1
{
  LocalAddr ALL
  RemoteAddr ALL
  LocalPortRangeRef portR1
  RemotePortRangeRef portR2
  Direction Inbound
  Priority 255
  TTLGroupActionRef gAct1~TN3270-Server
  TTLEnvironmentActionRef eAct1~TN3270-Server
}
TTLGroupAction gAct1~TN3270-Server
{
  TTLEnabled On
}
```

#6 - Secure Your Internal Network

```
TTLSEnvironmentAction eAct1~TN3270-Server
{
  HandshakeRole Server
  EnvironmentUserInstance 0
  TLSKeyringParmsRef keyR~SYSA
  TTLSCipherParmsRef cipher1~AT-TLS__Platinum
  TTLSEnvironmentAdvancedParmsRef eAdv1~TN3270-Server
}
TTLSEnvironmentAdvancedParms          eAdv1~TN3270-Server
{
  ApplicationControlled                On
  HandshakeTimeout                    10
  SecondaryMap                          Off
  SSLv3                                On
  TLSv1                                On
  TLSv1.1                              On
  TLSv1.2                                On
}
```

#6 - Secure Your Internal Network

TTLSTKeyringParms

keyR~SYSA

{

Keyring

TCPIPRing1

}

TTLSCipherParms

cipher1~AT-TLS__Platinum

{

V3CipherSuites

TLS_DH_DSS_WITH_AES_256_GCM_SHA384

V3CipherSuites

TLS_DHE_DSS_WITH_AES_256_GCM_SHA384

V3CipherSuites

TLS_DH_RSA_WITH_AES_256_GCM_SHA384

V3CipherSuites

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

V3CipherSuites

TLS_RSA_WITH_AES_256_GCM_SHA384

V3CipherSuites

TLS_RSA_WITH_AES_256_CBC_SHA

V3CipherSuites

TLS_RSA_WITH_AES_128_CBC_SHA

V3CipherSuites

TLS_RSA_WITH_DES_CBC_SHA

}

#6 - Secure Your Internal Network

```
##
## The last three cipher suites are required for legacy devices. They
## can be removed when those devices no longer exist.
##
PortRange portR1
{
  Port 992
}
PortRange portR2
{
  Port 1024-65535
}
```

#6 - Secure Your Internal Network

- Sample PAGENT proc in TCPIP.SEZAINST(PAGENT)
- Can run "as-is", will use /etc/pagent.conf as input
- Create userid and STARTED class profile from samples in TCPIP.SEZAINST(EZARACF):

```
AU PAGENT OWNER(SYS1) NOPASSWORD NAME('PAGENT STARTED TASK') +  
    OMVS(UID(0) HOME('/') PROGRAM('/bin/sh'))  
RDEFINE STARTED PAGENT.* OWNER(SYS1) UACC(NONE) +  
    STDATA(USER(PAGENT) GROUP(SYS1))  
SETROPTS RACLIST(STARTED) REFRESH
```



#6 - Secure Your Internal Network

- SERVAUTH class profiles required to grant access to TLS
- Format EZB.INITSTACK.<sysname>.TCPIP
- Grant READ authority for started task id's requiring TLS
- Define for TCPIP-related tasks
 - TCPIP, PAGENT, TN3270, FTPSERVE, PORTMAP, LPSERVE
 - NFS
 - CICS
 - DB2 DIST regions
 - MQ MSTR's and CHIN's, Qpasa
 - CA-ESP job scheduler
 - OPENSSEH
 - SYSLOGD
 - CSSMTP
 - Etc. (your site may have other tasks needing this profile)

#6 - Secure Your Internal Network

```
RDEFINE SERVAUTH EZB.INITSTACK.SYSA.TCPIP UACC(NONE) OWNER(SYS1)
      FROM(EZB.INITSTACK.SYST.TCPIP)
RDEFINE SERVAUTH EZB.INITSTACK.SYSB.TCPIP UACC(NONE) OWNER(SYS1)
      FROM(EZB.INITSTACK.SYST.TCPIP)
SETROPTS RACLIST(SERVAUTH) REFRESH
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(CICSA1)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(DB2P)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(MQPRCHIN)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(MQPRMSTR)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(QPMON)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(TCPIP)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(TN3270E)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(FTPSERVE)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(PAGENT)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(NFS)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(OPENSSH)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(SYSLOGD)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(LPSEVE)
PE EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH) AC(R) ID(PORTMAP)
SETROPTS RACLIST(SERVAUTH) REFRESH
```

#6 - Secure Your Internal Network

- Don't forget to create these profiles
- Handy reminders if you do forget:

```
EZD1313I REQUIRED SAF SERVAUTH PROFILE NOT FOUND 840  
EZB.INITSTACK.SYSA.TCPIP
```

```
ICH408I USER(TN3270 ) GROUP(SYS1 ) NAME(TN3270 SERVER )  
EZB.INITSTACK.SYSA.TCPIP CL(SERVAUTH)  
INSUFFICIENT ACCESS AUTHORITY  
ACCESS INTENT(READ ) ACCESS ALLOWED(NONE )
```

```
EZZ6011I TN3270E BPX1SOC FAILED, RC = 00000070 RSN = 74580296
```




#6 - Secure Your Internal Network

- You can issue OBEYFILE commands to implement
 - S PAGENT
 - OBEYFILE TCPIP PROFILE
 - OBEYFILE TN3270 PROFILE
- Don't forget to change TCPIP and TN3270 proc

#6 - Secure Your Internal Network

- Create TCPIP and TN3270 procs for both AT-TLS and non-AT-TLS
 - Symbol &M in proc

```
//TCPIP      PROC PARMS='CTRACE(CTIEZB00) ',M=AT
...
//PROFILE   DD DISP=SHR,DSN=SYS1.PARMLIB(PROFIL&M)

//TN3270    PROC PARMS='CTRACE(CTIEZBTN) ',M=AT
...
//PROFILE   DD DISP=SHR,DSN=SYS1.PARMLIB(TN3270&M)
```

- PROFILA0 for non-AT-TLS and PROFILAT for AT-TLS
- TN3270A0 for non-AT-TLS and TN3720AT for AT-TLS



#5 - Users With Elevated Authority

- RACF SPECIAL, OPERATIONS, AUDIT, ROAUDIT, Group-SPECIAL, Group-Operations, Group-Audit, Group AUTH, TRUSTED, PRIVILEGED, etc.
- CA-ACF2 SECURITY, AUDITOR, NON-CNCL, NOMAXVIO, LEADER, MAINT, etc.
- CA-TopSecret MSA, etc.
- Review users with this access and reduce or eliminate as appropriate
- Document business need for remaining users to have elevated authorities



#5 - Users With Elevated Authority

- SPECIAL, OPERATIONS, NON-CNCL, etc., access reports should also be reviewed daily
- If access appropriate, create profiles/rules to grant access
- Why Tom, who cares?
- Two benefits
 - From an audit perspective, access is more clearly documented after profile/rule is created
 - Performance improves with profile/rule
 - Decisions to grant SPECIAL, OPERATIONS, NON-CNCL, etc., access occur at very end of access decision tree in ESM



#5 - Users With Elevated Authority

- RACF ICETOOL reports
 - CONN - User IDs with group privileges above USE
 - UGLB - User IDs With extraordinary system-level authorities (SPECIAL, OPERATIONS, AUDITOR)
 - UGRP - User IDs with extraordinary RACF group authorities (Group-SPECIAL, Group-OPERATIONS, Group-AUDITOR)
 - OPER - Accesses allowed because user has OPERATIONS authority
 - SPEC - Events that succeeded because user has SPECIAL authority
- IBM presentation for remediating privileged users
 - [The Privileged User - Your Biggest Vulnerability?](#)



#5 - Users With Elevated Authority

- Unfortunately, RACF does not audit SUPERUSER access
- Simple test to show this
 - Enter 3.17, and select file you can't edit
 - Enable SUPERUSER, then edit file
 - Dump SMF and run IRRADU00 to dump audit records
 - This access is not audited
- Please vote for following RFE's
 - **Enhance Type 80s so I can tell when a UNIX authority that requires UID(0) was actually used (92188)**
 - **Provide logging of interactive superuser activities (63655)**
 - **Superuser Auditability (48290)**



#4 - Unix System Services Security

- Unix System Services (USS) security is largely misunderstood by many security administrators
- Many facets to USS security and a full discussion is beyond scope of this presentation
- Resources for further research
 - [z/OS UNIX User and File Security](#) by Eric Rosenfeld, IBM
 - [RACF UNIXPRIV Class](#) by Bob Hansel, RSH Consulting
 - [z/OS UNIX Systems Services Security Best Practices](#) by Vivian Morabito, IBM



#4 - Unix System Services Security

- Biggest exposure in USS Security is indiscriminate use of UID(0)
- UID(0) should not be used in user's OMVS segment
- For flesh-and-blood users, grant READ to FACILITY class profile BPX.SUPERUSER instead
 - Allows SU in Unix shell
 - Allows Enable Superuser in UDLIST (ISPF 3.17) or ISHELL
- For started task or batch id, review product install doc to determine if access to BPX.SUPERUSER should be granted
- If IBM or ISV insists on UID(0), tell them to use BPX.SUPERUSER instead



#3 - Inadequate RACF Database Controls

- Many sites use UACC(READ) for RACF databases
- Users don't need READ access to RACF database
- System calls RACF and RACF accesses database
- READ access allows users to download RACF database to PC
 - Password cracking tools such as John the Ripper can brute-force crack RACF encryption fairly easily (difficult to impossible after OA43998, OA43999)
- To remediate, change to UACC(NONE)
 - Grant READ or higher access to sysprogs, security admins, or production batch jobs running RACF database utilities
 - With V2R2, IRRDBU00 no longer requires UPDATE for NOLOCKINPUT, UPDATE still required for LOCKINPUT or UNLOCKINPUT

#3 - Inadequate RACF Database Controls

- RACF profiles to protect RACF database (assume SYS1.RACFPRIM and SYS1.RACFBKUP for primary and secondary database)

```
ADDSD SYS1.RACF* GEN OWNER(SYS1) UACC(NONE)
```

```
PE SYS1.RACF* GEN ID(SYSPROG) ACC(ALTER)
```

```
PE SYS1.RACF* GEN ID(IRRDDBU00) ACC(UPDATE)
```

- Some sites only allow ALTER to RACF when needed to allocate new RACF database (e.g. when installing new release of z/OS)



#2 - Inadequate Password Controls

- "For those of you still using 8-character passwords, all uppercase, no passphrases, no Multi-Factor Authentication, thank you"
 - Philip Young - SHARE in Sacramento
- Consider mixed-case passwords
 - Implementation problematic
 - Backout to uppercase renders mixed-case passwords unusable
- Consider passphrases
 - Greatly increases password security
 - Requires user education and commitment to change long-standing behavior
- Consider Multi-Factor Authentication
 - Easiest to implement and strongest method of authentication



#2 - Inadequate Password Controls

- Force password length to eight (8) characters
- Do anything possible to increase password keyspace and make brute force attack harder
- Inhibitors to implementation
 - Communication of password syntax changes to users
 - Update password rules for provisioners like ISIM, etc.



#2 - Inadequate Password Controls

- Use INACTIVE to revoke inactive users (e.g. 60 days)
- Use INTERVAL to require new password (e.g. 30 days)
- Keep 6-12 history entries to prevent password reuse
- REVOKE user after incorrect passwords (e.g. 3)
- Users without password INTERVAL whose passwords never expire and are not PROTECTED (RACF) or RESTRICT (CA-ACF2) are an exposure
- Such IDs should be batch or started task, not requiring password
- If you really need userid with non-expiring password
 - Limit ID's access to the bare minimum required to do the job
 - Be sure to document business case



#2 - Inadequate Password Controls - KDFAES

- OA43998 and OA43999 for RACF enabled much stronger password encryption (KDFAES) and added special characters to increase password keyspace
- You should implement KDFAES as soon as possible!
- Implementing KDFAES in RACF is simple
 - `SETR PASSWORD (ALGORITHM (KDFAES))`
- Backing out KDFAES in RACF is also simple
 - `SETR PASSWORD NOALGORITHM`
- RACF automatically determines correct format of password hash for current/historical password
 - RACF development did things right, no excuse for not implementing KDFAES

#2 - Inadequate Password Controls - KDFAES

- You should implement KDFAES as soon as possible!
- An excellent reference is [Joel Tilton's KDFAES Walkabout](#)
- Biggest issue for implementing KDFAES is performance
- KDFAES will increase CPU spent on password encryption
 - Enable VLF caching for all RACF structures
 - Run REPORT MISSINGFIX for these FIXCATs
 - IBM.Function.RACF.PasswordCharacters
 - IBM.Function.RACF.PasswordEncryption
 - Selectively convert current passwords to minimize performance issues
 - Selectively convert/delete historic passwords to minimize performance issues

#2 - Inadequate Password Controls - KDFAES

- KDFAES maintenance per II14765 (performance APARs in **BOLD**):
 - OA54190 - ICH408I FOR SOME VALID USERID/PASSWORD COMBINATIONS
 - OA53242 - INVALID PASSWORD MIXEDCASE KDFAES PASSASIS=OFF
 - **OA52291** - EXTRANEIOUS PURGE OF IRRACEE FROM FAILED COFCREAT
 - **OA52226** - RACF VLF PURGE IRRACEE FOR USER PROFILE CHANGES
 - **OA52117** - RACF KDFAES PERFORMANCE, OPTIMIZE VLF CACHE
 - OA50846 - ABEND0C4-11 IRRFRN00 OR ICH408I INVALID PASSWORD
 - OA50749 - SAF MACRO SUPPORT FOR RACF APAR OA50748
 - **OA50748** - MINIMIZE KDFAES PERFORMANCE IMPACTS
 - OA49494 - IRR420I ERROR 116 ABEND483 RSN088 ICHRIN00 KDFAES
 - **PI64443, PI64442, PI64175** - INCREASED CPU FOR PASSWORD VERIFICATIONS IN CICS AFTER KDFAES



AND THE #1 z/OS SECURITY ISSUE...

- Any guesses???



#1 - Inadequate APF Dataset Controls

- APF datasets are the "crown jewels" in z/OS
- Authorized code in APF dataset can do anything
- If hacker can get malicious code into an APF dataset, GAME OVER!
(Update your resume ☹)
- APF datasets should be audited for all successful UPDATE access and failed read access
- By auditing SUCCESSES(UPDATE), any changes to APF will be tracked via RACF SMF records
- For CA-ACF2, WRITE and ALLOCATE access will be logged with W(L) and A(L)
- For CA-TopSecret, CREATE, UPDATE, WRITE, and SCRATCH access will be AUDITed



#1 - Inadequate APF Dataset Controls

- Each APF dataset should be protected by fully-qualified generic profile in RACF (or equivalent in CA-ACF2 and CA-TopSecret)
 - Self-documenting
 - Prevents higher-level generic profile/rule from granting potentially inappropriate access
- CSV_APF_EXISTS health check should **NEVER** be an EXCEPTION
 - Why is this a LOW severity health check, IBM?
- If hacker can allocate non-existent APF dataset and plant malicious code, GAME OVER!
- Immediately remove APF dataset entry and issue SET PROG=xx or SETPROG command to clean up
- If SETPROG used, be sure to modify PROGxx for next IPL

#1 - Inadequate APF Dataset Controls

- APF datasets should be protected in RACF by fully-qualified generic profile with:

```
AUDIT (SUCSESSES (UPDATE) , FAILURES (READ) )
```

- Fully-qualified generic profile for APF dataset SYS1.LINKLIB in PROGxx:

```
APF ADD DSNAME (SYS1.LINKLIB) VOLUME (*****)
```

created with these commands:

```
ADDSD SYS1.LINKLIB GEN OWNER (SYS1) UACC (READ) -  
      AUDIT (SUCSESSES (UPDATE) , FAILURES (READ) )  
PE SYS1.LINKLIB GEN ID (SYSPROG) ACC (ALTER)
```

#1 - Inadequate APF Dataset Controls

- APF datasets should be protected in ACF2 by fully-qualified key with:

```
$KEY (SYS1)
```

```
LINKLIB UID (SYSPROG) R (A) W (L) A (L)
```

```
LINKLIB UID (*) R (A) W (P) A (P)
```

- Fully-qualified key is self-documenting
- WRITE and ALLOCATE accesses are tracked via ACF2 logging
- CSV_APF_EXISTS health check should NEVER be an EXCEPTION; fix IMMEDIATELY if it is

#1 - Inadequate APF Dataset Controls

- APF datasets should be protected in Top Secret with following commands:

```
TSS ADDTO (SYS1) DSNAME (SYS1.LINKLIB)
```

```
TSS ADDTO (AUDIT) DATASET (SYS1.LINKLIB) ACCESS (CREATE, UPDATE, WRITE, SCRATCH)
```

```
TSS PERMIT (SYSPROG) DSNAME (SYS1.LINKLIB) ACCESS (ALL)
```

```
TSS PERMIT (ALL) DSNAME (SYS1.LINKLIB) ACCESS (READ)
```

- Fully-qualified key is self-documenting
- CREATE, UPDATE, WRITE, and SCRATCH accesses are tracked with Top Secret AUDIT logging
- CSV_APF_EXISTS health check should NEVER be an EXCEPTION; fix IMMEDIATELY if it is



#1 - Inadequate APF Dataset Controls

- Often overlooked are TSO authorized programs in IKJTSOxx
- For commands/programs listed in AUTHCMD, AUTHPGM, and AUTHTSF sections, ensure that:
 - They exist
 - They are correct commands/programs in expected libraries
 - They are properly protected (UPDATE, ALLOC tightly controlled and audited)
- Also overlooked are APF-authorized programs in Unix filesystems
 - BPX.FILEATTR.APF controls who can set APF extended attribute bit
 - Use extattr command to set APF bit (e.g. extattr -a /user/sbin/proga)
 - Use find command to show APF-authorized programs (e.g. find / -ext a)



Finally...

- Please fill out an evaluation, your comments help me to deliver a better presentation
- I'm interested in hearing about your security experiences, positive or negative; if you encounter any unique situations or problems regarding security, or if you have questions, please let me know about them by sending an Email to pincons@rochester.rr.com