Configuring and Tuning SSH/SFTP on z/OS

Kirk Wolf
Stephen Goetze
Dovetailed Technologies, LLC

Tuesday, August 5, 2014: 4:15 PM-5:15 PM
Session 15497

www.dovetail.com

#SHAREorg

Copyright © 2014 Dovetailed Technologies, LLC

Dovetailed Technologies

We provide z/OS customers world wide with innovative solutions that enhance and transform traditional mainframe workloads:

- Co:Z Co-Processing Toolkit for z/OS

  z/OS Enabled SFTP, z/OS Hybrid Batch, z/OS Unix Batch integration

- JZOS

  acquired by IBM in 2005 and now part of the z/OS Java SDK

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Agenda

- What is SSH and how does it work with SFTP?
- IBM Ported Tools for z/OS – OpenSSH
  - Service planning and installation
  - Language environment tuning
  - Exploiting crypto hardware on z/OS
    - Using `/dev/random`
    - Hardware accelerated Ciphers and MACs
- Using IBM Ported Tools OpenSSH with Co:Z SFTP

➢ This presentation will cover selected topics from:
Dovetailed Technologies: P.T. OpenSSH – "Quick Install Guide"

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

What is SSH?

- The IETF SSH-2 standard protocol (RFC 4251 etc)
- Features:
  - A secure (encrypted) connection over **one** TCP/IP socket between a client and a server
  - *Authentication of the user and host.*
  - (optional) LZ compression
  - Support for one or more simultaneous ***application channels*** over the same connection: terminal, sftp, command, port fwd, ...
- There are many compatible implementations
  - **OpenSSH** is by far the most popular; it is a default package on all Unix/Linux distributions
  - PuTTY is a popular free Windows client
  - Many commercial implementations…

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

What is “SFTP” ?

- It's not FTP
- It's not FTPS (FTP with SSL/TLS)
- It's the Secure Shell (SSH2 specification) for file transfer
  - A packet/message spec, not a command/api spec
  - Most SSH implementations include an **sftp** command that has subcommands familiar to FTP users
  - The SFTP and FTPS wire protocols are **not** compatible

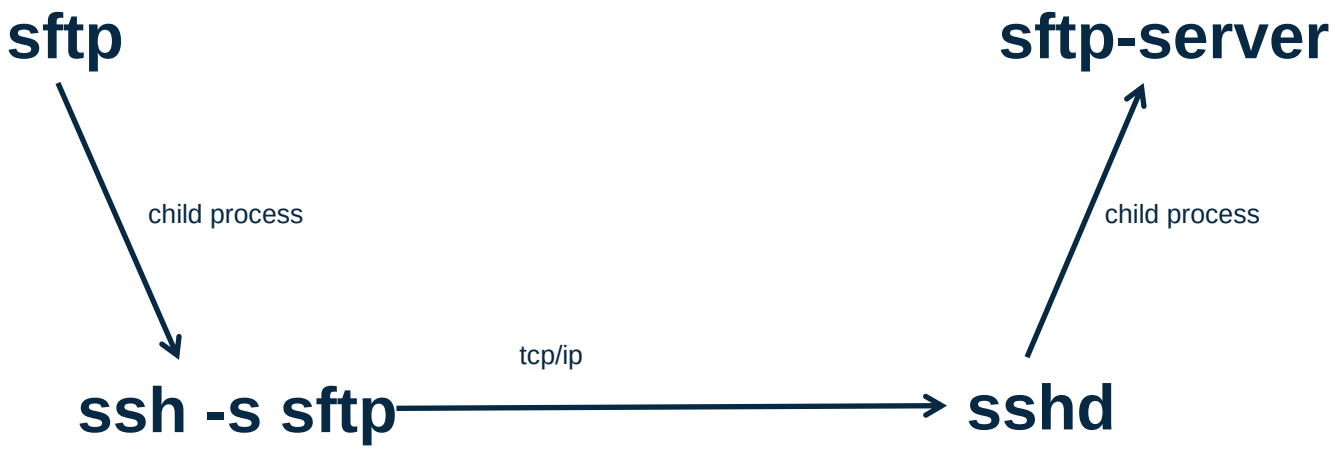
➢ SFTP is an SSH “application/subsystem”

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

SFTP as an SSH Application/Subsystem



Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval
Copyright 2014 Dovetailed Technologies
Copyright © 2014 Dovetailed Technologies, LLC

IBM Ported Tools for z/OS - OpenSSH

- IBM's port of OpenSSH for z/OS
  - z/OS Unix commands: **ssh, sshd, sftp, sftp-server**, etc.
  - Supports password and key authentication
  - ***No*** sftp support for MVS datasets, spool files, etc.
- Release 1.2 added support for:
  - SSH keys in SAF/RACF keyrings
  - SMF logging (new SMF 119 record subtypes)
- PTF UA63842 added:
  - ICSF hardware acceleration for Ciphers and MACs
- A no-charge z/OS product; normal IBM support

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Co:Z SFTP

Enhanced versions of OpenSSH **sftp** and **sftp-server** commands for z/OS.

- Relies on IBM Ported Tools OpenSSH for “ssh” layer.
- Compatible with non-z/OS implementations of SSH SFTP (follows the “ssh-filexfer” spec)
- Adds support for z/OS datasets and spool files, with flexible control over:
  - Dataset allocation, DCB attributes, etc
  - Codepage conversion, Line-termination rules,
  - Record padding, overflow, etc.
- Support for listing catalogs, PDS directories, and JES spool files
- SMF 119 records that are compatible with IBM FTP
- IBM FTP-compatible user exits
- Free to use under our “Community License”
  - Enterprise License and Support agreements are also available

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

SFTP tuning and crypto HW exploitation

- When using SFTP + SSH, often 90% of the CPU time is in SSH.
  - After all, that is where all of the encryption and TCP/IP processing occurs.
  - This is true regardless of whether you use IBM P.T. sftp or Co:Z SFTP

- We need to focus on IBM Ported Tools OpenSSH tuning and crypto hardware exploitation in order to save CPU and optimize throughput.
- With tuning, SSH/SFTP resource consumption is about the same as FTPS.

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

IBM Ported Tools OpenSSH Prerequisites for crypto exploitation

- z/OS 1.10 or later
- CPACF - processor feature 3863 (free and enabled by default in most countries)
- ICSF installed and running (even if you don't have a co-processor card)
  - CPACF instructions are used by ICSF for Ciphers and MACS
  - HCR77A0 ("A0" level) and later has support for /dev/random without crypto card. Requires z/OS 1.12 or later.
  - HCF77A1 (“A1” level) adds support for bypassing SAF checks on random number and hash APIs.

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Service Planning

- "IBM Ported Tools for z/OS" 5665-M23 1.2.0 HOS1120
  - See Upgrade: PORTED4ZOS Subset: HOS1120
  - Be sure to include PTF UA63842
- If running on z/OS 1.10 or z/OS 1.11, check that the PTFs for APARs PK86329 and OA29401 have been applied
- Review and install as appropriate ICSF and its required service.

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

LE Tuning Recommendations

- Ported Tools OpenSSH uses LE XPLINK runtime libraries (like Java, WebSphere, etc)

  See: "Placing Language Environment Modules in LPA .."
  - Add SCEELPA to LPALST
  - Add SCEERUN and SCEERUN2 to LNKLST
  - SCEERUN and SCEERUN2 should be program controlled
  - Implement samples CEE.SCEESAMP(CEEWLPA) and (EDCWLPA) as shipped

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval
Copyright 2014 Dovetailed Technologies
Copyright © 2014 Dovetailed Technologies, LLC

SSH2 Crypto at-a-glance

- ***"Key Exchange"***

  At start of session, RSA or DSS server key pair is used with Diffie-Hellman exchange and MAC (usually SHA-1)
  - Authenticates the identity of the server
  - Generates and exchanges a secret "session key"
  - The session can be "rekeyed". Typically once/hour or GB.

- ***"User Auth"***

  At start of session, a password or ***user*** public key can be used to authenticate the user to the server.

➢ ***"Key Exchange"*** and ***"User Auth"*** are covered in detail in two Webinar recordings - see References.

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

SSH2 Crypto at-a-glance (cont.)

- ***"Transport"***
  - A MAC algorithm (typically SHA-1) is used to generate a hash of each packet.
  - A symmetric Cipher uses the shared session key to encrypt the packet payload.

➢ Since this happens for *each* packet, it can be ***expensive.*** This session will focus on tuning the ***"Transport"***

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Using ICSF and /dev/random

- Each SSH client or server session requires secure random numbers (a.k.a “entropy”)
- Ported Tools OpenSSH will use `/dev/random` if the ICSF CSFRNG service is available. The alternative (ssh-rand-helper) is slow and not particularly secure.
  - using `/dev/random` can save a couple of seconds at the beginning of each SSH or SFTP session.
- Prior to ICSF HCR77A0, ICSF CSFRNG required a co-processor card, but this is no longer true

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Using ICSF and /dev/random (cont.)

- Simply need to allow required users access to ICSF CSFRNG service. For most environments, this can be granted to all:

```
RDEFINE CSFSERV CSFRNG UACC(NONE)
PERMIT CSFRNG CLASS(CSFSERV) ID(*) ACCESS(READ)
SETROPTS RACLIST(CSFSERV) REFRESH
```

Note: You must authorize both SSHD server userids.

To test (from a normal z/OS user UNIX shell):

```
$ head /dev/random | od -x
```


Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Enabling ICSF Ciphers and MACs

- Cryptographic Ciphers (encryption) and MACs are where lots of CPU cycles can be spent. P.T. OpenSSH will use ICSF and CPACF instructions if available, which can reduce overall CPU usage by > 50%.
- The following CSFSERV profiles control access:
  - CSFIQA - ICSF Query Algorithm
  - CSF1TRC - PKCS #11 Token record create
  - CSF1TRD - PKCS #11 Token record delete
  - CSF1SKE - PKCS #11 Secret key encrypt
  - CSF1SKD - PKCS #11 Secret key decrypt
  - CSFOWH - One-Way Hash Generate

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval
Copyright 2014 Dovetailed Technologies
Copyright © 2014 Dovetailed Technologies, LLC

Enabling ICSF Ciphers and MACs (cont.)

```
RDEFINE CSFIQA  CLASS(CSFSERV) UACC(NONE)
RDEFINE CSF1TRC CLASS(CSFSERV) UACC(NONE)
RDEFINE CSF1TRD CLASS(CSFSERV) UACC(NONE)
RDEFINE CSF1SKE CLASS(CSFSERV) UACC(NONE)
RDEFINE CSF1SKD CLASS(CSFSERV) UACC(NONE)
RDEFINE CSFOWH  CLASS(CSFSERV) UACC(NONE)
/* permit all, some users, or a group:  */
PERMIT  CSFIQA  CLASS(CSFSERV) ID(*) ACCESS(READ)
...
SETROPTS CLASSACT(CSFSERV)
SETROPTS RACLIST(CSFSERV) REFRESH
```

Note: You must authorize all client/server end userids as well as both SSHD server userids.

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Enabling ICSF Ciphers and MACs (cont.)

Possible ICSF HCR77A0 or later gotcha:

Avoid defining the following specific or generic SAF/RACF profile that matches:

```
CLASS(CRYPTOZ) CLEARKEY.SYSTOK-SESSION-ONLY
```

- *If a match is not found - no problem*
- *If a match **is** found, then y*ou must grant all client/server end userids as well as both SSHD server userids READ access.

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Enabling ICSF Ciphers and MACs (cont.)

To configure client and server to use ICSF Ciphers and MACs support, update both `/etc/ssh/zos_ssh_config` and `/etc/ssh/zos_sshd_config`:

```
# Use either software or ICSF for Ciphers and MACs
CiphersSource any
MACsSource any
```


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

HCR77A1 performance enhancement option

```
RDEFINE CSF.CSFSERV.AUTH.CSFOWH.DISABLE
    CLASS(XFACILIT) UACC(READ)
RDEFINE CSF.CSFSERV.AUTH.CSFRNG.DISABLE
    CLASS(XFACILIT) UACC(READ)
SETROPTS CLASSACT(XFACILIT)
SETROPTS RACLIST(XFACILIT) REFRESH
```

Defining these profiles in the XFACILIT class will disable SAF/RACF checks for CSFOWH (hash) and CSFRNG (random number) APIs.

Since ICSF uses CPACF instructions for these anyway (which can't be protected by SAF/RACF), this is usually an acceptable option.

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

SSH Cipher and MAC negotiation

- The default Ciphers and MACs list supported by P.T. OpenSSH (commented out in `/etc/ssh/ssh_config` and `/etc/ssh/sshd_config`) –

```
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,
arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,
aes192-cbc,aes256-cbc,arcfour,
rijndael-cbc@lysator.liu.se

# MACs hmac-md5,hmac-sha1,umac-64@openssh.com,
hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96
```


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

SSH Cipher and MAC negotiation (cont.)

- The following Ciphers and MACs will be accelerated by ICSF and CPACF –

```
Ciphers aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc

MACs hmac-sha1,hmac-sha1-96
```

Note: Some older z machines do not support aes-192 and aes-256 (see below).

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

SSH Cipher and MAC negotiation (cont.)

- SSH client and server ***negotiate*** which Cipher and MAC to use for the session.

- ***RULE:***
  Use the first algorithm in the client list that appears anywhere in the server list.

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Configure z/OS SSH *client* Ciphers and MACs

- Update `/etc/ssh/ssh_config`
- Strategy #1: Only support accelerated Ciphers. SHA-1 is fine for MACs.

```
Ciphers aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc
MACs hmac-sha1,hmac-sha1-96
```

- Strategy #2: Prefer accelerated Ciphers; fall back to all others. (move preferred to front of list)

```
Ciphers aes128-cbc,aes192-cbc,aes256-
cbc,3des-cbc,<others from default list>
MACs hmac-sha1,hmac-sha1-96
```


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Configure z/OS SSHD *server* Ciphers and MACs

- Update `/etc/ssh/sshd_config`
- Strategy #1: Only allow accelerated Ciphers; others will fail. SHA-1 is fine for MACs.

```
Ciphers aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc
MACs hmac-sha1,hmac-sha1-96
```

- Strategy #2: Allow any Cipher; coordinate with client to use an accelerated Cipher. SHA-1 is fine for MACs.

```
# Ciphers <use default config>
MACs hmac-sha1,hmac-sha1-96
```


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Verify ICSF setup

- Login remotely to an z/OS ssh shell session so that we can use the ssh client (which is not allowed under TSO OMVS)

```
zos$ ssh -vvv myuser@127.0.0.1
```

…

```
debug2: ------------------------------------
debug2: CRYPTO    SIZE      KEY       SOURCE
debug2: ------------------------------------
debug2: AES       256       SECURE    COP
debug2: AES       256       SECURE    CPU
debug2: DES       56        SECURE    COP
debug2: DES       56        SECURE    CPU
```


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Verify ICSF setup (cont.)

```
…
debug2: MD5       128       NA        SW
debug2: SHA-1     160       NA        CPU
debug2: TDES      168       SECURE    COP
Debug2: TDES      168       SECURE    CPU
```

Note: SOURCE=CPU means CPACF, which is what ICSF uses for SSH Cipher and MAC acceleration.

Note: The strength/size is the largest bit length supported by the facility. In the display above, AES-128, AES-192, and AES-256 are supported via ICSF with CPACF.

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Verify ICSF setup (cont.)

…

```
debug3: RNG is ready, skipping seeding
```

Note: This message implies that `/dev/random` was used for initializing random numbers.

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Verify ICSF setup (cont.)

…

```
debug1: mac_setup_by_id: hmac-sha1 from source ICSF
debug2: mac_setup: found hmac-sha1
debug1: zsshIcsfMacInit (402): CSFPTRC successful:
return code = 0, reason code = 0, handle = 'SYSTOK-
SESSION-ONLY                00000000S   '
```

Note: These messages indicate that ICSF was used for MAC hmac-sha1

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Verify ICSF setup (cont.)

…

```
debug1: cipher_init: aes128-cbc from source ICSF
debug1: zsshIcsfCipherInit (930): CSFPTRC successful:
return code = 0, reason code = 0, handle = 'SYSTOK-
SESSION-ONLY                 00000001S   '
```

Note: These messages indicate that ICSF was used for Cipher aes128-cbc

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC

Measuring resource consumption

- With cozsftp client, COZ_LOG=D will print ssh CPU time
  - `-oMACsSource=OpenSSL -oCiphersSource=OpenSSL` can be used to disable ICSF for a single client session
- (harder): look at SMF30 completion records –
  Client:
  - AS #1: (JES init) + COZBATCH + Co:Z SFTP
  - AS #2: (OMVS) /bin/ssh

  Server:
  - AS #1: (OMVS) sshd process for the session
  - AS #2: (OMVS) /bin/sh -c sftp-server.sh
  - AS #3: (OMVS) sftp-server (P.T. or Co:Z version)

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval
Copyright 2014 Dovetailed Technologies
Copyright © 2014 Dovetailed Technologies, LLC

Using Co:Z SFTP client with IBM Ported Tools OpenSSH

- Simply invoke the “cozsftp” command instead of “sftp”:

Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval
Copyright 2014 Dovetailed Technologies
Copyright © 2014 Dovetailed Technologies, LLC

Using Co:Z SFTP server with IBM Ported Tools SSHD

- Update `/etc/ssh/sshd_config`

```
#Subsystem  sftp /usr/lib/ssh/sftp-server
Subsystem   sftp /u/vendor/coz/bin/sftp-server.sh
```

The Co:Z supplied sftp-server.sh shell script will by default still invoke the IBM sftp-server unless user has a Co:Z SFTP server profile. Sites can make Co:Z SFTP the default via this change:

```
# file: /etc/ssh/sftp-server.rc
…
USE_COZ_SFTP=true
```


Copyright 2014 Dovetailed Technologies
Copyright © 2014 Dovetailed Technologies, LLC

References

- IBM Ported Tools for z/OS: OpenSSH
  - User's Guide
    http://www-03.ibm.com/systems/resources/fot4os02.pdf

- IBM Ported Tools OpenSSH - Quick Install Guide
  http://dovetail.com/docs/pt-quick-inst/index.html

- Dovetail webinar recordings:
  - IBM Ported Tools OpenSSH – Key Authentication
  - IBM Ported Tools OpenSSH – Using Key Rings

Copyright 2014 Dovetailed Technologies

Copyright © 2014 Dovetailed Technologies, LLC