What's New in z/OS OpenSSH V2R4

Kirk Wolf
Steve Goetze
info@dovetail.com

Trademarks

- Co:Z® is a registered trademark of Dovetailed Technologies, LLC
- z/OS® is a registered trademark of IBM Corporation
- Windows, PowerShell are trademarks of Microsoft Corporation

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 – Uses IBM z/OS OpenSSH
  - z/OS Enabled SFTP
  - z/OS Hybrid Batch
  - z/OS Unix Batch Integration
  - z/OS Remote Services

- JZOS – acquired by IBM and now part of the z/OS Java SDK

Agenda

- What is SSH?
- Review major releases:
  - z/OS V2R3 OpenSSH
  - z/OS V2R4 OpenSSH
- Migration considerations

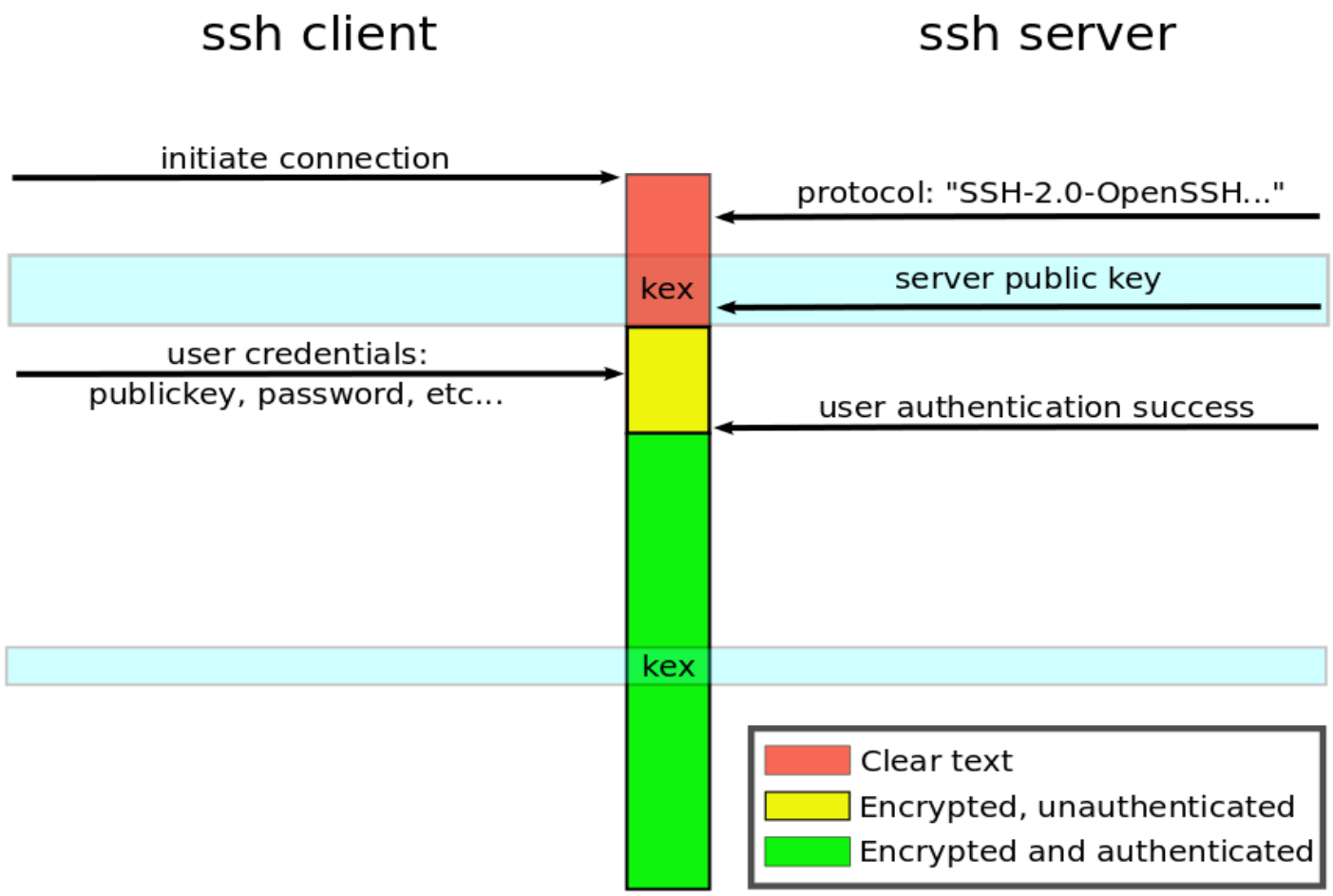
What is SSH?

- Original freeware version developed by Tatu Ylönen (1995)
- The IETF SSH-2 standard protocol (RFC 4251 etc) (2006)
- Features
  - A secure (encrypted) connection over one TCP/IP socket between a client and a server
  - Authentication of both user and host(server)
  - (optional) LZ compression
- Support for one or more simultaneous application channels over the same connection: terminal, sftp, command, port forwarding, ...
- There are many compatible implementations
  - OpenSSH (1999) is by far the most popular; it is a default package on all Unix/Linux distributions. Also available from Microsoft for Windows and PowerShell.
  - PuTTY is a popular free Windows client

SSH2 Crypto at-a-glance

- Key Exchange – “kex”
  - Some variant of the Diffie-Hellman algorithm
  - Client generated random number and the server key are used to
    - Allow the client to authenticate the identity of the server
    - Cooperatively generate and exchange a secret session key
    - Supports session rekeying. Typically once/hour or GB
- User Authentication
  - At start of session, a password or user key pair can be used to authenticate the user to the server
- Session Encryption
  - A symmetric Cipher uses the shared session key to encrypt the packet payload
  - An HMAC algorithm (typically HMAC-SHA-x) is used to generate a secure hash of each packet

SSH Encryption and Authentication



Dovetailed Technologies

IBM z/OS OpenSSH - Versions

- IBM z/OS V2R2 OpenSSH
  - V2.2.0 – HOS2220 – z/OS 2.2 - OpenSSH 6.4p1
- IBM z/OS V2R3 OpenSSH
  - **V2.3.0 – HOS2230 – z/OS 2.3 - OpenSSH 6.4p1**
- IBM z/OS V2R4 OpenSSH
  - **V2.4.0 – HOS2240 – z/OS 2.4 - OpenSSH 7.6p1**

Dovetailed Technologies

IBM z/OS V2R3 OpenSSH – Change Summary

- CPACF Support
  - V2R3 with APAR OA54299 installed enables IBM z/OS OpenSSH to directly use CPACF instructions, when present, to implement symmetric ciphers and MAC algorithms
- zERT Support
  - Updated to be a Cryptographic Protocol Provider for z/OS Encryption Readiness Technology (zERT)

Dovetailed Technologies

IBM z/OS V2R4 OpenSSH – New Feature Summary

- Base upgraded from OpenSSH 6.4p1 to 7.6p1
- KeyRing keys now use Systems SSL for signature creation and verification
- Support ECDSA keys stored in KeyRings
- Added new cryptography algorithms
  - Key exchange (KEX)
  - Cipher
  - User/host Keys
- Added ssh-proxyc for ssh clients to connect using SOCKS5 proxy servers
- Enhanced SMF Type 119 subtype 94 and 95 to identify connection IP address and port

Dovetailed Technologies

IBM z/OS V2R4 OpenSSH – New Features

- **Upgraded from OpenSSH 6.4p1 (released November 2013) to OpenSSH 7.6p1 (released October 2017)**
  - Security patches and bug fixes through OpenSSH 7.8p1 also included
- KeyRing keys now use Systems SSL for signature creation and verification
  - SSH keys (both user and host) stored in KeyRings now use Systems SSL and ICSF for all operations
  - Private key material for these keys may now be stored in ICSF on crypto cards
  - May require permitting users access to algorithm resources in the CSFSERV class if using KeyRing keys and these RACF resources are defined
- Support ECDSA keys (user and host) in z/OS KeyRings and with FIPS
  - Customers can use ECDSA keys with the additional security of KeyRing and ICSF
  - Includes the ability to store private key material in crypto cards

IBM z/OS V2R4 OpenSSH – New Features

- **Key Exchange algorithms** (listed in default preference order):
  - ✓ **curve25519-sha256**
  - ✓ **curve25519-sha256@libssh.org**
  - ✓ ecdh-sha2-nistp256*
  - ✓ ecdh-sha2-nistp384*
  - ✓ ecdh-sha2-nistp521*
  - ✓ diffie-hellman-group-exchange-sha256*
  - ✓ **diffie-hellman-group16-sha512**
  - ✓ **diffie-hellman-group18-sha512**
  - ✓ diffie-hellman-group-exchange-sha1*
  - ✓ **diffie-hellman-group14-sha256**
  - ✓ diffie-hellman-group14-sha1*

Bold = new with z/OS V2.4 (in OpenSSH 7.6.1)

* = supported by ICSF

- The list of available kex algorithms may be obtained using "ssh -Q kex"

Dovetailed Technologies

IBM z/OS V2R4 OpenSSH – New Features

- **Key algorithms** - used for ssh host(server) or user keys (listed in default preference order):
  - ✓ ecdsa-sha2-nistp256-cert-v01@openssh.com
  - ✓ ecdsa-sha2-nistp384-cert-v01@openssh.com
  - ✓ ecdsa-sha2-nistp521-cert-v01@openssh.com
  - ✓ **ssh-ed25519-cert-v01@openssh.com**
  - ✓ ssh-rsa-cert-v01@openssh.com
  - ✓ ecdsa-sha2-nistp256 *
  - ✓ ecdsa-sha2-nistp384 *
  - ✓ ecdsa-sha2-nistp521 *
  - ✓ **ssh-ed25519**
  - ✓ ssh-rsa *
  - ✓ ssh-dss * (Note: DSA keys now disabled by default)

Bold = new with z/OS V2.4 (in OpenSSH 7.6.1)
* = KeyRing (w/ICSF) support

ed25519 is a elliptic curve signature scheme that offers better security than ECDSA and DSA and good performance.

- The list of available key algorithms may be obtained using "ssh -Q key"

IBM z/OS V2R4 OpenSSH – New Features

- Cipher algorithms (listed in default preference order):
  - ✓ **chacha20-poly1305@openssh.com**
  - ✓ aes128-ctr *#
  - ✓ aes192-ctr *#
  - ✓ aes256-ctr *#
  - ✓ aes128-gcm@openssh.com
  - ✓ aes256-gcm@openssh.com
  - ✓ aes*-cbc *# (present in /sample)

Bold = new with z/OS V2.4 (in OpenSSH 7.6.1)

* = supported by ICSF

\# = supported using CPACF instructions

chacha20-poly1305@openssh.com combines Daniel Bernstein's ChaCha20 stream cipher and Poly1305 MAC to build an authenticated encryption mode

- The list of available Cipher algorithms may be obtained using "ssh -Q cipher"
- **Note:** this order has been changed in the /sample configurations to prefer CPACF ciphers.

Dovetailed Technologies

IBM z/OS V2R4 OpenSSH – New Features

- Mac algorithms (listed in default preference order):
  - ✓ hmac-sha2-256-etm@openssh.com *#
  - ✓ hmac-sha2-512-etm@openssh.com *#
  - ✓ hmac-sha1-etm@openssh.com *#
  - ✓ hmac-sha2-256 *#
  - ✓ hmac-sha2-512 *#
  - ✓ hmac-sha1 *#
  - ✓ umac-64-etm@openssh.com
  - ✓ umac-128-etm@openssh.com
  - ✓ umac-64@openssh.com
  - ✓ umac-128@openssh.com
  - ✓

* = supported by ICSF
= supported using direct CPACF instructions

- The list of available MAC algorithms may be obtained using "ssh -Q mac"

IBM z/OS V2R4 OpenSSH – New Features

- Added a new proxy client command for use with the SSH client to navigate through a SOCKS proxy
  - Command name: ssh-proxyc
  - Used with the previously available SSH client “ProxyCommand” option
  - “ProxyFDPass yes” must specified in the ssh command

  - Example usage:
    - # In /etc/ssh/ssh_config or user .ssh/config file
    - Host ahost-behind-proxy.mydomain.com
    - ProxyCommand /usr/bin/ssh-proxyc -p socksproxy.mydomain.com:8080 %h %p
    - ProxyUseFDPass yes
    - Host *
    - …

IBM z/OS V2R4 OpenSSH – New Features

- Added the IP address and port to the SMF Type 119 “connection started” records (subtype 94, 95)
  - A new triplet section has been added to these subtypes
  - Allow customers to audit IP addresses for both successful and failed connections

Dovetailed Technologies

IBM z/OS V2R4 OpenSSH – Installation Notes

- New release (HOS2240) is included as base element in V2R4
- ICSF is required on pre-z14 machines for /dev/random and if ICSF crypto routines are used
- Verifying version
  - $ ssh -V
  - OpenSSH_7.6p1, OpenSSL 1.0.2h 3 May 2016
  - $ /usr/sbin/sshd -d -t
  - debug1: sshd version OpenSSH_7.6, OpenSSL 1.0.2h 3 May 2016

IBM z/OS V2R4 OpenSSH – Migration Considerations

- **No longer supported:**

- SSH Protocol version 1 is no longer supported (This has been disabled in the default configuration since HOS1130)
- Running without SSHD privilege separation is no longer supported (was already the default since HOS1120)
- Support for legacy v00 OpenSSH certs removed
- No longer supports pre-authentication compression by sshd. SSH clients will either need to support delayed compression or otherwise compression will not be negotiated for the session
- Removed support for Blowish and RC4 ciphers and the RIPE-MD160 HMAC (Hash authentication), specifically blowfish-cbc, cast128-cbc, arcfour, arcfour128, arcfour256, hmac-ripemd160, and hmac-ripemd160@openssh.com
- No longer supports RSA keys smaller than 1024 bits

Dovetailed Technologies

IBM z/OS V2R4 OpenSSH – Migration Considerations

- The following options are no longer enabled by default:
  - root login using a password
  - Support for the 1024-bit Diffie Hellman key exchange, specifically: diffie-hellman-group1-sha1
  - Support for MD5-based and truncated MD5 and SHA1 HMAC algorithms, specifically: hmac-md5, hmac-md5-96@openssh.com, hmac-sha1-96@openssh.com, hmac-md5-etm@openssh.com, hmacmd5-96-etm@openssh.com, hmac-sha1-96-etm@openssh.com
  - Support for the Triple DES cipher, specifically: 3des-cbc
  - Support for DSA (dss) user and host keys are no longer enabled by default (see more following)

IBM z/OS V2R4 OpenSSH – Migration Considerations

- **Authentication using key rings is done using ICSF**
  - This requires that you permit SAF/RACF read access to several algorithm resources in the CSFSERV class (**if they have been defined**)

    ✓ CSFIQA, CSF1TRC, CSF1TRD, CSF1PKS, CSF1PKV, CSF1DVK, CSF1GAV

  - If you have a cryptographic coprocessor card installed, then you must also permit read access to the following CSFSERV resources (**if they are defined**)

    ▪ CSFDSG, CLSFDSV, CSFPKI

IBM z/OS V2R4 OpenSSH – Migration Considerations

- **/etc/ssh/moduli configuration file**
  - Changed to support new group-exchange KEX algorithms with larger group sizes
  - Customers should copy /samples/moduli to /etc/ssh/moduli
    - Otherwise the use of these algorithms with larger groups will result in a long delay during connection to construct the new group

IBM z/OS V2R4 OpenSSH – Migration Considerations

- **Support for DSA (dss) user and host keys are no longer enabled by default**
  - To continue use, enable them by adding the following to /etc/ssh/ssh_config and /etc/ssh/sshd_config, or $HOME/.ssh/config file:
    - PubkeyAcceptedKeyTypes +ssh-dss
    - HostKeyAlgorithms +ssh-dss

IBM z/OS V2R4 OpenSSH – Migration Considerations

- **SSHD “UseDNS” option**
  - The default value for the UseDNS option changed from "yes" to "no"
  - With this change, sshd no longer converts a client's IP address back into a host name. This prevents the use of hostnames in Host match blocks in the configuration file, also causes host-based authentication to fail (which is not enabled by default)
  - Note: This option is re-enabled in /samples/sshd_config for compatibility, but you may want to disable this so as to avoid DNS lookups during login

IBM z/OS V2R4 OpenSSH – Migration Considerations

- **New/updated configuration options and updated sample configuration files**
  - Review existing configuration files (/etc/ssh/ssh_config, /etc/ssh/, sshd_config, /etc/ssh/zos_ssh_config, /etc/ssh/zos_sshd_config) to determine applicability of new features or the use of obsolete options.
  - Many new configuration options have been added through OpenSSH 7.6, and defaults for others have been changed
  - Customers should consider implementing the new versions of these configuration files in /samples
- **Perform the following steps.**
  1. Copy the updated /samples/moduli to /etc/ssh/moduli
  2. Compare their current ssh(d)_config and zos_ssh(d)_config files with the new /samples and review the differences. Pay particular attention to uncommented options in the current installed configuration files that have changed or are obsolete.
  3. Add or change options as required for the installation (based on your previous settings)
  4. Test the new installation and configuration
  5. See the User's Guide, "OpenSSH files" for more information on configuration options.

IBM z/OS V2R4 OpenSSH – Migration Considerations

- **ICSF usage and sample configuration files**

  - ✓ With this release (and feature extensions in previous V2R3 PTFs), most customers will not need to use ICSF for Ciphers and MACs. The defaults and sample configuration files will prefer and automatically use direct CPACF implementations for these algorithms, which will generally result in the best performance.

IBM z/OS V2R4 OpenSSH – Migration Considerations

- **Migration Health Check**
  - ✓ APAR OA57724 provides a Health Check that can be used with z/OS V2R3 to check your default system configuration files for possible usage of features that are obsolete.

- **Consider zERT as part of your migration**
  - ✓ Customers with many OpenSSH connections that use varied configuration options may wish to use zERT to collection SMF 119 records that can be audited to see which connections are being made and what algorithms they are using. Popular SMF reporting tools include zERT SMF 119 record support.

IBM z/OS V2R4 OpenSSH – Configuration and Tuning

- **Our guide for setup and tuning z/OS OpenSSH**
  - Common install customization path
  - ICSF (for /dev/random)
  - LE tuning
  - etc.

  ✓ **“IBM z/OS OpenSSH - Quick Install Guide”**

  ✓ http://dovetail.com/docs/pt-quick-inst/index.html

Dovetailed Technologies

IBM z/OS V2R4 OpenSSH – Publications

- z/OS OpenSSH V2R4 User's Guide: SC27-6806-40
- z/OS V2R4 Announcement letter
- z/OS V2R3 Statement of Direction: ENYS 217-536

Dovetailed Technologies

IBM z/OS V2R4 OpenSSH – References

- OpenSSH - http://www.openssh.org/
- OpenSSL - http://www.openssl.org/
- Dovetailed Technologies:

  http://dovetail.com
- http://dovetail.com/docs/pt-quick-inst/index.html

  “z/OS OpenSSH Quick Install Guide”