SSH Client Suite for z/VSE and VSE^n

Neale Ferguson
Sine Nomine Associates

Overview

SINE NOMINE ASSOCIATES

- A look at the technologies involved in bringing the SSH Clients to z/VSE and their capabilities
- Tony Thigpen's session on Friday at 15:30 will provide a user perspective on the clients

Agenda

- What's in it
- Technology
  - Hardware acceleration when available
  - C-based built on z/VM
  - File Systems
  - Codepage support
  - Auditing & Tracing
  - Security options
- Limitations
- Future

What is it?

SINE NOMINE ASSOCIATES

- Fork of PuTTY
- Fork of CMS SSH
- 3 main clients
  - SNAPTERM: Secure Shell
  - SNAPSFTP: Secure File Transfer
  - SNAPSCP: Secure Copy
- Uses z/Architecture cipher instructions if available

Hardware Acceleration

SINE NOMINE ASSOCIATES

- Detects availability of hardware facilities
- Uses instructions such as:
  - km/kmt/kmctr – ciphers
  - kimd/klmd – message digests
- Falls back to software if not available
- Future plan includes adding ECC-related accelerations

Hardware Acceleration – An Aside

SINE NOMINE ASSOCIATES

- It is unpredictable whether any new function code added in the message-security-assist extension 3 or higher is supported by the following instructions:
  - CIPHER MESSAGE
  - CIPHER MESSAGE WITH CHAINING
  - COMPUTE INTERMEDIATE MESSAGE DIGEST
  - COMPUTE LAST MESSAGE DIGEST

Runtime Detection…

SINE NOMINE ASSOCIATES

```
         XC    MSACAP,MSACAP      Assume MSA is not available
         LHI   R0,L'STFLEWRK/8    Size of output area
         LA    R8,STFLEWRK        Get A(Output Area)
         STFLE STFLEWRK           Get all facilities
         IF (TM,FACB2,MSABIT,O)   If MSA available
*        ---------------------
            OC    MSACAP,=Y(MSALVL1)   Set indicator
         ENDIF
*        -----
         IF (TM,FACB9,MSA3BIT,O)  If MSA 3 is available
*        ----------------------
            OC    MSACAP,=Y(MSALVL2+MSALVL3) Set indicator
         ENDIF
*        -----
         EPSW  R0,R1               Inspect PSW
         IF (TMLH,R0,ESAMODE,Z)    If we're in zArch mode
*        ---------------------
            IF (TM,FACB9,MSA4BIT,O)   If there's MSA4
*           ----------------------
               OC    MSACAP,=Y(MSALVL4)  Set indicator
            ENDIF
*           -----
            SPACE 1
            IF (TM,FACB7,MSA4BIT,O)   If there's MSA5
*           ----------------------
               OC    MSACAP,=Y(MSALVL5)   Set indicator
```

…Runtime Detection…

SINE NOMINE ASSOCIATES

- Each cipher implementation can check if a particular algorithm is supported by using the query operand which returns a bitmap:

```
kmc - f0 70 38 38 00 00 00 00 10 00 00 00 00 00 00 00
kmt - f0 70 38 38 00 00 00 00 00 00 00 00 00 00 00 00
```

- Each bit corresponds to the operand code for the algorithm e.g. KMT_AES_256 is bit 20

…Runtime Detection

SINE NOMINE ASSOCIATES

```
Initialised AES-256 SDCTR (System Z accelerated) outbound encryption
Initialised HMAC-SHA-256 (System Z accelerated) outbound MAC algorithm
Initialised AES-256 SDCTR (System Z accelerated) inbound encryption
Initialised HMAC-SHA-256 (System Z accelerated) inbound MAC algorithm
```

```
Initialised AES-256 SDCTR (unaccelerated) outbound encryption
Initialised HMAC-SHA-256 (System Z accelerated) outbound MAC algorithm
Initialised AES-256 SDCTR (unaccelerated) inbound encryption
Initialised HMAC-SHA-256 (System Z accelerated) inbound MAC algorithm
```

C based – with Some Assembler

SINE NOMINE ASSOCIATES

- z/VM and VSE compilers don't support `__asm__` type statements
- z/OS does but it's clumsier than gcc
- Use assembler code and call it from C using LE conventions

C based – with Some Assembler

SINE NOMINE ASSOCIATES

```
#pragma inline(kmc_query)
static int
kmc_query(km_function_t code)
{
    km_status_t stat;
    int res;

    KMCQRY(&stat);

    res = stat[code / 8] & (1 << (7 - (code % 8)));

    return (res != 0);
}
```

```
KMCQRY   CEEENTRY PPA=PPAAREA,AUTO=WORKSIZE,MAIN=NO,NAB=YES
:
         IF (TMLL,R15,MSALVL1,O)  If MSA available?
*        ------------------------
            LHI   R0,0               Get query code
            KMC   R4,R2              Perform KMC
         ENDIF
*        -----
:
         CEETERM
```

File Systems

SINE NOMINE ASSOCIATES

- Standard VSE Files: DD:<[*d*|*t*]*lbl name*>
- VSE devices: <DD:SYS*xxx*>
- VSAM: DD:<*dlbl name*>
- LIBR: DD:<*lib*>.<*sublib*>(<*member*>)
- Memory Files: <*filename*>
- Future – POWER?

File Systems – Standard

SINE NOMINE ASSOCIATES

```
// DLBL FTP2TXT,'TEST.DATA.2',,SD
// EXTENT SYS001,SYSWK1,,,49700,20
// EXEC SNAPSCP,SIZE=SNAPSCP,                                          -
               PARM='-l neale -i DD:KEYFILE -lrecl 80 -recfm f ',     -
               PARM='-batch_accept -blksize 8000 ',                   -
               PARM='-tr 172.17.16.43:test.data DD:FTP2TXT'

// EXEC SNAPTERM,SIZE=SNAPTERM,                                        -
               PARM='-l neale -batch_accept -i DD:KEYFILE ',          -
               PARM='cts7xdev.devlab.sinenomine.net ',                -
               PARM='-sshlog DD:SYSLST pwd'
```

File Systems – VSAM

SINE NOMINE ASSOCIATES

```
// DLBL FTP2TXT,'TEST.DATA.2',,VSAM
// EXTENT SYS001,SYSWK1,,,49700,20
// EXEC SNAPSCP,SIZE=SNAPSCP,                                    -
               PARM='-l neale -i DD:KEYFILE -lrecl 80 -recfm f ',  -
               PARM='-batch_accept -blksize 8000 ',                -
               PARM='-tr 172.17.16.43:test.data DD:FTP2TXT'

// DLBL HOSTKEY,'VSESSH.HOSTKEY.CLUSTER',,VSAM
:
 DEFINE CLUSTER(                          -
  NAME(VSESSH.HOSTKEY.CLUSTER)            -
  RECORDSIZE(677, 677)                    -
:
  INDEXED                                 -
  REUSE                                   -
 )                                        -
 INDEX(                                   -
  NAME(VSESSH.HOSTKEY.INDEX)              -
 )                                        -
 DATA(                                    -
  NAME(VSESSH.HOSTKEY.DATA)               -
 )                                        -
 CATALOG(VSESP.USER.CATALOG)
```

File Systems – LIBR

SINE NOMINE ASSOCIATES

```
// DLBL BATCH,'PSFTP.BATCH',,SD
// EXTENT SYS001,SYSWK1
:
// EXEC SNAPSFTP,SIZE=SNAPSFTP,                                    -
               PARM='-l neale -batch_accept -i DD:PRD2.SSHV2(MY.KEY) ',-
               PARM='-b DD:BATCH -bc ',                            -
               PARM='cts7xdev.devlab.sinenomine.net'


site --codepage iso8859-1:ibm-1047 --lrecl 80 --recfm f
cd /home/neale
get libr.job DD:PRD2.SSHV2(LIBR.JOB)
```

File Systems – Memory Files

SINE NOMINE ASSOCIATES

```
// EXEC SNAPSFTP,SIZE=SNAPSFTP,                                    -
               PARM='-l neale -batch_accept -i DD:KEYFILE ',       -
               PARM='-b DD:SYSIPT -bc ',                           -
               PARM='cts7xdev.devlab.sinenomine.net'
site --codepage iso8859-1:ibm-1047 --lrecl 80 --recfm f
cd /home/neale
get libr.job memory.file
put memory.file memory.file
exit
/*
```

Codepage Support

- Default ASCII<->EBCDIC

```
// EXEC SNAPSCP,SIZE=SNAPSCP,                                          -
               PARM='-l neale -i DD:KEYFILE -lrecl 80 -recfm f ',      -
               PARM='-batch_accept -blksize 8000 ',                    -
               PARM='-tr 172.17.16.43:test.data DD:FTP2TXT'
```

- Any codepage supported by iconv()

```
site --codepage iso8859-1:ibm-1047 --lrecl 80 --recfm f
cd /home/neale
get libr.job DD:PRD2.SSHV2(LIBR.JOB)
```

```
// EXEC SNAPSCP,SIZE=SNAPSCP,                                          -
               PARM='-l neale -i DD:KEYFILE -lrecl 80 -recfm f ',      -
               PARM='-batch_accept -cp iso8859-1:ibm-1047 ',           -
               PARM='172.17.16.43:test.data DD:FTP2TXT'
```

Logical Units

- SYSIPT – stdin
- SYS002 – stdout/stderr*
- SYS003 – stderr*

```
int rc = getSysParm("STDERR  ", stderrDD, 80);
conControl->input = fopen("DD:SYSIPT","r");
conControl->out->stream = fopen("DD:SYS002", "wb,recfm=v,lrecl=133,type=record");
            /*
             * User has specified // SETPARM STDERR= so we set up a separate stream for it
             */
if (rc == 0) {
   conControl->err->stream = fopen((const char *) stderrDD,
                                   "wb,recfm=v,lrecl=133,type=record");
```

Analysis of Running a Job…

SINE NOMINE ASSOCIATES

```
// JOB PSFTP
// SETPARM STDERR='DD:ERRORS'
// LIBDEF PHASE,SEARCH=(PRD2.SSHV2,PRD2.TCPIPB)
// ASSGN SYS001,DISK,VOL=SYSWK1,SHR
// DLBL SSHPKEY,'VSESSHV2.KEY'
// EXTENT SYS001,SYSWK1
// DLBL HOSTKEY,'VSESSH.HOSTKEY.CLUSTER',,VSAM,CAT=IJSYSUC
// DLBL KEYFILE,'ECDSA.NEW',,SD
// EXTENT SYS001,SYSWK1
// DLBL LIBRJOB,'DD.LIBR.JOB',,SD
// EXTENT SYS001,SYSWK1,,,49730,1000
// ASSGN SYSIPT,SYSRDR
// ASSGN SYS002,SYSLST
// ASSGN SYS003,DISK,VOL=SYSWK1,SHR
// DLBL ERRORS,'PSFTP.STDERR',,SD
// EXTENT SYS003,SYSWK1,,,49680,20
```

…Analysis of Running a Job…


```
// EXEC SNAPSFTP,SIZE=SNAPSFTP,                                    -
               PARM='-l neale -batch_accept -i DD:KEYFILE ',       -
               PARM='-b DD:SYSIPT -bc ',                           -
               PARM='cts7xdev.devlab.sinenomine.net'
cd /tmp
ls
site --codepage iso8859-1:ibm-1047 --lrecl 80 --recfm f
cd /home/neale
get libr.job DD:PRD2.SSHV2(LIBR.JOB)
site --codepage iso8859-1:ibm-1047 --lrecl 80 --recfm f
get libr.job LIBR.JOB
site --codepage iso8859-1:ibm-1047 --lrecl 80 --recfm f --blksize 16000
get test.data DD:LIBRJOB
site --codepage iso8859-1:ibm-1047 --lrecl 80 --recfm f
put DD:HOSTKEY vse.keys
site --binary --lrecl 80 --recfm f
put DD:PRD2.SSHV2(CMDGEN.O) cmdgen.object
rm libr.job.bin
pwd
exit
/*
/&
```

…Analysis of Running a Job…

SINE NOMINE ASSOCIATES

```
1S54I  PHASE SNAPSFTP IS TO BE FETCHED FROM PRD2.SSHV2
Using username "neale".

Remote working directory is /home/neale
psftp>
cd /tmp
Remote directory is now /tmp
psftp>
ls
Listing directory /tmp
drwxrwxrwt    8 root     root          172 May 21 04:07 .
dr-xr-xr-x   18 root     root          235 Oct  7  2019 ..
drwxrwxrwt    2 root     root            6 Oct 20  2017 .font-unix
drwxrwxrwt    2 root     root            6 Oct 20  2017 .ICE-unix
drwxrwxrwt    2 root     root            6 Oct 20  2017 .Test-unix
drwxrwxrwt    2 root     root            6 Oct 20  2017 .XIM-unix
drwxrwxrwt    2 root     root            6 Oct 20  2017 .X11-unix
drwx------    3 root     root           17 Feb 21 19:26 systemd-private
psftp>
site --codepage iso8859-1:ibm-1047 --lrecl 80 --recfm f
psftp>
cd /home/neale
Remote directory is now /home/neale
psftp>
get libr.job DD:PRD2.SSHV2(LIBR.JOB)
remote:/home/neale/libr.job => local:DD:PRD2.SSHV2(LIBR.JOB)
psftp>
```

…Analysis of Running a Job…

SINE NOMINE ASSOCIATES

```
site --codepage iso8859-1:ibm-1047 --lrecl 80 --recfm f
psftp>
get libr.job LIBR.JOB
remote:/home/neale/libr.job => local:LIBR.JOB
psftp>
site --codepage iso8859-1:ibm-1047 --lrecl 80 --recfm f --blksize 16000
psftp>
get test.data DD:LIBRJOB
remote:/home/neale/test.data => local:DD:LIBRJOB
psftp>
site --codepage iso8859-1:ibm-1047 --lrecl 80 --recfm f
psftp>
put DD:HOSTKEY vse.keys
local:DD:HOSTKEY => remote:/home/neale/vse.keys
psftp>
site --binary --lrecl 80 --recfm f
psftp>
put DD:PRD2.SSHV2(CMDGEN.O) cmdgen.object
local:DD:PRD2.SSHV2(CMDGEN.O) => remote:/home/neale/cmdgen.object
psftp>
rm libr.job.bin
rm /home/neale/libr.job.bin: no such file or directory
1S55I  LAST RETURN CODE WAS 0008
EOJ PSFTP     MAX.RETURN CODE=0008
```

…Analysis of Running a Job…

```
BG 0000 4933D EQUAL FILE ID IN VTOC  ERRORS   SYS003=A81  SYSWK1
   PSFTP.STDERR
BG-0000
0 delete
BG 0000 SNAPSFTP (c) Sine Nomine Assocates - Starting
BG 0000 SNAPSFTP Writing to DD:PRD2.SSHV2(LIBR.JOB) - PRD2.SSHV2(LIBR.JOB)
BG 0000 SNAPSFTP Writing to LIBR.JOB - PSFTP.LIBR.JOB
BG 0000 4933D EQUAL FILE ID IN VTOC  LIBRJOB  SYS001=A81  SYSWK1
   DD.LIBR.JOB
BG-0000
0 delete
BG 0000 SNAPSFTP Writing to DD:LIBRJOB - DD.LIBR.JOB
BG 0000 SNAPSFTP Reading from DD:HOSTKEY - VSESSH.HOSTKEY.CLUSTER
BG 0000 SNAPSFTP Reading from DD:PRD2.SSHV2(CMDGEN.O) - PRD2.SSHV2(CMDGEN.O)
BG 0000 SNAPSFTP terminating
BG 0000 EOJ PSFTP     MAX.RETURN CODE=0008
        DATE 05/21/2023, CLOCK 10/18/54, DURATION   00/04/17
```

Auditing

SINE NOMINE ASSOCIATES

- All file openings are logged to the console

```
BG 0000 SNAPSFTP Writing to DD:LIBRJOB - DD.LIBR.JOB
BG 0000 SNAPSFTP Reading from DD:HOSTKEY - VSESSH.HOSTKEY.CLUSTER
BG 0000 SNAPSFTP Reading from DD:PRD2.SSHV2(CMDGEN.O) - PRD2.SSHV2(CMDGEN.O)
BG 0000 SNAPSFTP terminating
BG 0000 EOJ PSFTP     MAX.RETURN CODE=0008
        DATE 05/21/2023, CLOCK 10/18/54, DURATION   00/04/17
```

Tracing…

- All commands have a verbose option -v

```
Looking up host "cts7xdev.devlab.sinenomine.net" for SSH connection
Connecting to 172.17.16.43 port 22
We claim version: SSH-2.0-PuTTY_CMS
Remote version: SSH-2.0-OpenSSH_7.4
Using SSH protocol version 2
Doing ECDH key exchange with curve Curve25519 and hash SHA-256 (System Z accelerated)
Server also has ecdsa-sha2-nistp256/ssh-rsa host keys, but we don't know any of them
Host key fingerprint is:
ssh-ed25519 255 60:c4:27:07:d1:56:6a:88:c6:45:89:cc:f6:02:23:4e
Initialised AES-256 SDCTR (System Z accelerated) outbound encryption
Initialised HMAC-SHA-256 (System Z accelerated) outbound MAC algorithm
Initialised AES-256 SDCTR (System Z accelerated) inbound encryption
Initialised HMAC-SHA-256 (System Z accelerated) inbound MAC algorithm
Reading key file "DD:KEYFILE"
Using username "neale".

Offered public key
Offer of public key accepted
Authenticating with public key "ed25519-key-20230201"
Passphrase for key "ed25519-key-20230201":
Sent public key signature
Access granted
Opening main session channel
Opened main channel
Started a shell/command
Session sent command exit status 0
/home/neale
Main session channel closed
All channels closed
```

…Tracing…

- Use `-sshlog` or `-sshrawlog` for packet tracing:

```
// EXEC SNAPTERM,SIZE=SNAPTERM,                                    -
               PARM='-l neale -batch_accept -i DD:KEYFILE ',       -
               PARM='cts7xdev.devlab.sinenomine.net ',             -
               PARM='-sshlog DD:SYSLST pwd'
```

…Tracing

SINE NOMINE ASSOCIATES

```
=~=~=~=~=~=~=~=~=~=~=~=~=~ PuTTY log 2023.05.21 15:00:52 =~=~=~=~=~=~=~=~=~=~=~=~=~
Event Log: Looking up host "cts7xdev.devlab.sinenomine.net" for SSH connection
Event Log: Connecting to 172.17.16.43 port 22
Event Log: We claim version: SSH-2.0-PuTTY_CMS
Event Log: Remote version: SSH-2.0-OpenSSH_7.4
Event Log: Using SSH protocol version 2
Mon May 21 15:00:52 2023 - Incoming packet
#0x0,
type 20 / 0x14 (SSH2_MSG_KEXINIT) (247D756)

  00000000  85 7f 00 38 8a 36 79 05 5b 71 df 26 97 ec b2 fe  ...8.6y.[q.&....|
  00000010  00 00 01 40 63 75 72 76 65 32 35 35 31 39 2d 73  ...@curve25519-s|
  00000020  68 61 32 35 36 2c 63 75 72 76 65 32 35 35 31 39  ha256,curve25519|
```

Security of Keys

SINE NOMINE ASSOCIATES

- Options include:
  - Do nothing
  - Basic Security Manager
  - External Security Manager

Security of Keys – Do Nothing…

SINE NOMINE ASSOCIATES

- No passphrase
  - Key file is just a file: DITTO/IDCAMS/…
- Passphrase
  - Access to disk containing key doesn't reveal usable key
  - Passphrase must be kept secure

```
// EXEC SNAPTERM,SIZE=SNAPTERM,                                    -
               PARM='-l neale -batch_accept -i DD:KEYFILE ',       -
               PARM='cts7xdev.devlab.sinenomine.net ',             -
               PARM='pwd'
Handle me with care
```

…Security of Keys – Do Nothing…

SINE NOMINE ASSOCIATES

- Generate key with passphrase

```
// EXEC    SNACMDGN,SIZE=*,                                    -
               PARM='-t ed25519 -b 256 -o DD:KEYFILE ',         -
               PARM='--new-passphrase DD:.SYSIPT'
Handle me with care
/*
// EXEC    SNACMDGN,SIZE=*,                                    -
               PARM='-O public-openssh -o DD:PUBLIC ',          -
               PARM='DD:KEYFILE’
```

- Using the passphrase

```
// EXEC SNAPTERM,SIZE=SNAPTERM,                                -
               PARM='-l neale -batch_accept -i DD:KEYFILE ',    -
               PARM='cts7xdev.devlab.sinenomine.net ',          -
               PARM='pwd'
Handle me with care
```

…Security of Keys – Do Nothing

SINE NOMINE ASSOCIATES

- Security of passphrase now becomes the problem
- It's just sitting there in the job stream or in a file

Security of Keys – BSM

SINE NOMINE ASSOCIATES

- Control Access to Files via `//  ID` card
- Use DTSECTAB to authorize access
- Doesn't help if device is accessible elsewhere: DDR from z/VM
- Too many years since I touched BSM

Security of Keys – ESM

SINE NOMINE ASSOCIATES

- Let the External Security Manager address the challenges of key protection

Limitations

SINE NOMINE ASSOCIATES

- Batch-only (at the moment)
- Unable to use the `scp` protocol as you need to supply a file size at the start
  - `sftp` protocol is the default anyway
- Build limitations:
  - C on z/VSE is too back-level
  - C on z/VM is better but still not as good as z/OS
  - Thank goodness LE conventions are the same
- VSE revealed a bug in VM's `selectex()`

Future

- ECC hardware assists
- POWER support
- Server
  - Is there a requirement
  - I have a prototype CMS server
  - z/VSE looks “straightforward”

QUESTIONS?