

SSL for VM: The Hard Way and the Easy Way

David Boyes

Agenda

- Overview of SSL and the VM Implementation
- Setup Steps for a DIY Version
- SSL Enabler, aka the Easy Way
- A Little Bit About Clients
- Q&A

What is SSL?

- Basic functions are:
 - A method of exchanging identification information between two communicating hosts
 - A method of exchanging protection requirements
 - A method of implementing encryption
 - A few miscellaneous management utilities related to the other functions
- Originated as WWW-specific, but has been extended as a mechanism for general TLS implementation
- Supports a number of different algorithms and methods of operation that can be scaled to fit different needs
- Reference Implementation is OpenSSL (openssl.org)

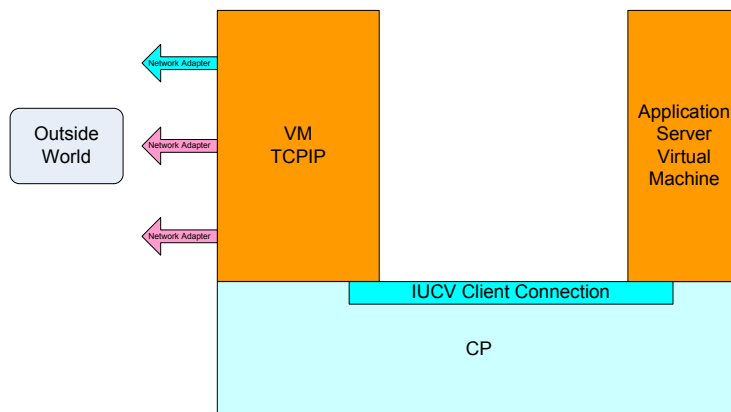
What is the Idea?

- Essentially the problem is how to add a transparent layer of authorization and encryption to any socket-based application. If we were doing this the “right way”, the application would need modification to adapt to the SSL TLS layer.
- The VM approach is equivalent to the ‘stunnel’ utility: the ability to wrap an application in a protected transport without requiring modifications to the application.
- This method works acceptably well for single-connection services like TELNET, HTTP and SMTP, but has problems with more complex protocols like FTP

The VM Implementation of SSL

- Introduced in z/VM 4.x
- The VM SSLSERV implementation provides a transparent wrapper service for any incoming TCP-based protocol.
- Implemented in a separate virtual machine (SSLSERV)
- Based on internal IBM implementation of SSL cribbed from Websphere, not the more common OpenSSL implementation
 - Does not benefit from improvements in SSL reference model
 - Does not benefit from crypto coprocessor enablement in OpenSSL
- Requires a Linux distribution to function (not included)

Normal Non-SSL Data Flow



Drawbacks of VM Implementation

- Only works on incoming connections
- Transparent implementation deprecated for FTP (and few clients support it)
- Currently limited to 128 sessions per SSLSERV machine/per stack (open APAR)
- Does not exploit crypto processors
- Does not support all popular authentication and encryption options
- Requires acquisition of Linux guest from outside source (not runnable out of the box from IBM)

Setup Steps

- Install a supported Linux guest
- Perform VM TCPIP Configuration Steps
- Locate SSLSERV RPMs
- Install RPM and Destroy Linux Normal TCP Stack Function
- Generate and Install Host Certificates
- Enable Secure Services for PORT Statement in PROFILE TCPIP

Install A Supported Linux Guest

- Currently “officially” supported for RHEL 4 and SLES 9 on both 31 and 64 bit distributions
 - Also works on Debian and Slack390 (with some work)
- SSLSERV expects a “default” install of either distribution PLUS the “compat” RPM to get an outdated version of the C and C++ libraries
 - Binaries are built on old release of SLES/RHEL to allow function on multiple releases, but C library release and internal API is dramatically different on newer distribution releases
- Guest may NOT be shared with any other purpose
- Guest must be installed using default SSLSERV directory entry and WITHOUT formatting 201 minidisk
- VDISK swap recommended for > 10-15 sessions

Update DTCPARMS File

- Create a SSLSERV DTCPARMS file on TCPMAINT 198:

```
:nick.SSLSERV :type.SERVER :class.SSL

:nick.SSL :type.CLASS
      :name.SSL Server
      :command.VMSSL
      :diskwarn.YES
      :parms.
```

SSLSERV Options You Care About

- MAXUSERS

Defines the maximum number of SSL protected sessions for this stack

- IPLDEVICE

Defines what device to IPL for the Linux guest.

- TRACE

Generates a LOT of output – use when requested only

All address/port specifications must be numeric IP addresses (bug!)

Update ETC SERVICES

- Add the description for the SSL administrative service:

```
ssladmin    9999/tcp          # SSL admin port
```

Enable Secure Service

- Add AUTOLOG and admin port statement for SSLSERV machine to PROFILE TCPIP

```
AUTOLOG
  SSLSERV 0 ; SSL Server
```

- Add PORT for SSL administration

```
PORT
  9999 TCP SSLSERV ; SSL admin
```

Locate SSLSERV RPMs

- SSLSERV RPMs shipped on 5VMTCP0 493 minidisk (for 5.2)
- Both “source” and precompiled binary RPMs supplied
 - The “source” RPM contains only partial source
- Make sure to get the right version for your distribution
 - If building your own appliance, start with the RH one – fewer prereqs to hunt down

Install RPMs and Destroy Linux TCP Stack

- Install the RPMs using 'rpm -i' from the command line
- **DO NOT LOG OFF THE LINUX GUEST UNTIL YOU FINISH THIS STEP**
 - The SSLSERV RPMs destroy the ability for the Linux guest to communicate with normal network adapters
 - Only existing connections survive the install, so unless you fancy doing the rest of the configuration with 'sed' on the 3270 console, you have to finish the job before you log out
- You'll also need to write a init script for the ssld daemon; the IBM package includes a sample, but it doesn't install it (and it doesn't work even if you do install it correctly). Use the template supplied with your distribution as a basis.

Generate and Install Host Certificate

- From TCPMAINT or other privileged user, use the SSLADMIN command to add certificates
- See description in chapter 22 of the TCPIP Planning and Configuration guide for detailed directions on certificate generation
- **Keep a backup copy of your certificate files! SSLSERV does not provide any way to extract, copy or renew certificates in place (planned for > z/VM 5.4)**

Enable Secure Services for PORT Statements

- Add the SECURE keyword to the PORT statements in PROFILE TCPIP that you want to protect.

PORT 25 SMTP (old)

PORT 25 SMTP **SECURE** (new)

- Can be done with OBEYFILE or by recycling the stack
- Smart to provide an alternate port until you're completely happy with the configuration (convention is to add 900 to the normal port number for the secure version of the service)

SNA Pre-assembled SSL Enabler

- After spending 4 and half weeks trying to get this to work, SNA put together a pre-configured Linux guest system for SSL enablement and provide it for download from <http://www.sinenomine.net/debian/ssl>
 - No charge (we just ask you to register so we can tell you when we update it)
 - Based on Debian (stripped down for appliance use only)
 - Install with CMSDDR
 - Full IBM-style installation documentation in text, PDF, and Bookmaster format.
 - All SSLSERV build, install and configuration steps completed up to the point of generating/installing certificates
 - Works on unsupported VM releases (known to work back to z/VM 3.1)
 - Support is available
- Not officially supported by IBM, but we've been able to work out most problems in concert with level 2 in Endicott
- AFAIK, the SSL Enabler system is the most widely deployed configuration of SSLSERV. Even IGS uses it instead of doing their own...8-)

About SSL-Enabled Clients

- Most clients can be supplied with a 'stunnel' wrapper, but this may limit authorization functions somewhat.
- Ports of stunnel are available for most operating systems (Windows, Linux (native), OS/2, etc)

FTP is Special

- Don't confuse SFTP with FTPS!
 - SFTP refers to the SSH File Transfer Protocol, NOT FTP over SSL
 - FTPS is FTP over SSL
- Two variants of FTPS
 - Implicit - Works with VM SSL
 - Explicit - Doesn't work with VM SSL
- Only a few clients support implicit FTPS.

Bluezone

- Very nicely implemented
- Good support for SSL and non-SSL connections
- Free download for testing, reasonable commercial price
- www.bluezone.com

Hummingbird

- Expensive, but complete
- Note difference between FTPS Implicit setting and FTPS Explicit. Default is Explicit
- Best integration with Windows Explorer
- www.hummingbird.com

X3270

- Open source 3270 emulation
- Runs on most popular OS
- Must be compiled with the `--with-SSL` option
 - Most Linux distributions now do this
- X3270.sourceforge.net

FTP Clients

- Linux “Just Works”; only `--implicitSSL` switch needed
- Most Windows FTP clients don’t work
- CMS FTP client doesn’t work (ask me about CMS FTP->FTPS proxy)

Common Browsers (IE, Firefox, Iceweasel)

- Browsers function as expected
- Make sure you read and understand the restrictions on client certificates if your WWW server application uses or expects them

H3270

- H3270.sourceforge.net
- Open source alternative to HOD or HATS – needs only a Javascript-capable browser on user device
- Doesn't do file transfer, but is much lighter weight, and can be offloaded to Linux on IFL for non-VM systems

Speculation/Opinion

- Comments from the IBM developers indicate that they're rethinking the design of the VM SSL server
 - CMS multitasking base instead of Linux
 - Certificate extract/copy capability
 - Crypto engine support
- This redesign is at least one release away. I'd really rather have them cooperate with the community to move to OpenSSL and an officially blessed appliance model

Summary

- VM can participate in a SSL world; it's just harder than necessary
- Help is available via the free SSL appliance SNA provides
- Practice safe computing; enable SSL today!

Q&A

Contact Info

David Boyes
Sine Nomine Associates
www.sinenomine.net
dboyes@sinenomine.net