CyaSSL Application Note

Tips for using CyaSSL on STM32 with LwIP and FreeRTOS

December, 2012
Version 1.0

1.0 Introduction

The CyaSSL embedded SSL library has been ported to both the LwIP TCP/IP stack as well as the FreeRTOS operating system. CyaSSL has been verified to run with this configuration and several tips are noted below.

2.0 Configuring CyaSSL

CyaSSL's custom build defines are located in the settings.h file, located at <cyassl_root>/ cyassl/ctaocrypt/settings.h. The following sections will reference necessary changes to this file when building for specific platform components.

A. LwIP

CyaSSL has support for LwIP when LwIP has been configured to use the Sockets API. To build CyaSSL with LwIP, define **CYASSL_LWIP** in settings.h. LwIP needs to be configured to use the Sockets API, which can be done by defining "LWIP_SOCKET 1" in lwip/opt.h or in the build.

B. FreeRTOS

To build CyaSSL with support for FreeRTOS, define **FREERTOS** in settings.h. By default, the FreeRTOS build disables writev, SHA-512, DH, DSA, and HC-128. The FreeRTOS build does have support for multithreaded applications if desired. If multithreading is not desired, define SINGLE_THREADED when building CyaSSL.

Copyright 2012 Sawtooth Consulting Limited. All rights reserved.

C. STM32

There are several other build settings which may need to be used when building CyaSSL on the STM32 platform. These may include:

SIZEOF_LONG_LONG 8

This sets the 64-bit type for CyaSSL. CyaSSL benefits speed-wise from having a 64-bit type available. Set **SIZEOF_LONG** or **SIZEOF_LONG_LONG** to match the result of sizeof(long) and sizeof(long long) on your platform.

NO_CYASSL_DIR

This will need to be defined if the dirent.h header is not available.

NO_DEV_RANDOM

CyaSSL's random number generator defaults to using /dev/random or /dev/urandom. If these are not available, **NO_DEV_RANDOM** will need to be defined. If defined, the user needs to write an OS-specific GenerateSeed() function (located in "ctaocrypt/src/random.c"). If you would like to use the STM32 hardware supported RNG with the STM32 standard peripheral library to get the random seed, please contact yaSSL at support@yassl.com.

NO_RABBIT

When tested last, the RABBIT stream cipher was not yet compatible with the STM32 platform when built with the Keil MDK-ARM. This define will disable the RABBIT stream cipher in CyaSSL.

3.0 Support

Please contact support@yassl.com with any questions or comments regarding using CyaSSL on the STM32 platform.

Copyright 2012 Sawtooth Consulting Limited. All rights reserved.