Open Source Internet Security

Company / Product Overview
October, 2016
ABOUT US

Founded: 2004

Location: Bozeman, MT
Seattle, WA
Portland, OR

Our Focus: Open Source Embedded Security
(for Applications, Devices, IoT, and the Cloud)

Products: - wolfSSL
- wolfSSL FIPS
- wolfCrypt
- wolfSSH
- wolfMQTT
- wolfSCEP
- wolfSSL Inspection
- yaSSL

© Copyright 2016 wolfSSL
wolfSSL is Growing!

- 3 employees in 2011
- 9 employees in 2012
- 11 employees in 2013
- 15 employees in 2014
- 19 employees in 2015

300 OEM Customers
15 Resale Partners

© Copyright 2016 wolfSSL
Industry Partnerships

ARM

Intel

Freescale

Marvell

Texas Instruments

Microchip

Samsung

Mentor Embedded

Green Hills Software

IAR Systems

NXP

Renesas

Atmel

Analog Devices

Wind

© Copyright 2016 wolfSSL
Currently Securing 2 Billion Connections!
WOLFSSL
Lightweight SSL / TLS Library

LIGHTWEIGHT. PORTABLE. C-BASED.

✓ Up to TLS 1.2 and DTLS 1.2
✓ 20-100 kB footprint
✓ 1-36 kB RAM per session
✓ Up to 20X Smaller than OpenSSL
✓ Long list of supported operating systems
✓ TLS 1.3 – Targeting Late 2016 (1st to Market)

Windows, Linux, Mac OS X, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded Linux, WinCE

Haiku, OpenWRT, iPhone (iOS), Android, Nintendo Wii and Gamecube through DevKitPro, QNX, MontaVista, NonStop

TRON/ITRON/uITRON, Micrium uC/OS, FreeRTOS, SaferRTOS, Freescale MQX, Nucleus, TinyOS, HP/UX, ARC MQX…

© Copyright 2016 wolfSSL
ADDITIONAL FEATURES:

- OpenSSL Compatibility Layer
- Web Server Integration
- Hardware Cryptography Support
  (STM32, Freescale Kinetis CAU/mmCAU, Coldfire, Microchip PIC32MZ, Cavium NITROX, Intel AES-NI/AVX1/AVX2/RDRAND/RDSEED)
- NSA Suite-B Compatible
- FIPS 140-2 Level 1 Validated

© Copyright 2016 wolfSSL
PORTABLE MODULAR CRYPTOGRAPHY

✓ Previously called “CTaoCrypt”
✓ Working on splitting into separate product
✓ Progressive list of supported ciphers
✓ Modular design, assembly optimizations

AES (CBC, CTR, CCM, GCM),
DES, 3DES, Camellia,
ARC4, RABBIT, HC-128, ChaCha20

MD2, MD4, MD5, SHA-1,
SHA-256, SHA-384, SHA-512,
BLAKE2b, RIPEMD-160, Poly1305

RSA, ECC, DSS, DH, EDH, NTRU
HMAC, PBKDF2, PKCS#5
ECDH-ECDSA, ECDHE-ECDSA,
ECDH-RSA, ECDHE-RSA,
Curve25519, Ed25519

© Copyright 2016 wolfSSL
Algorithms

MD2, MD4, MD5, SHA-1, SHA-2, SHA-3, RIPEMD
DES, 3DES, AES, Camellia
ARC4, RABBIT, HC-128, ChaCha20
AES-GCM, AES-CCM, Poly1305
RSA, ECC, DSS, DH, EDH
HMAC, PBKDF2

Hash Functions
Block Ciphers
Stream Ciphers
Authenticated Ciphers
Public Key Options
Password-based Key Derivation

© Copyright 2016 wolfSSL
BRINGING WOLFSSL TO JAVA USERS

✓ **JNI wrapper** around wolfSSL

✓ Full support for **DTLS 1.2**

  Current Java (including Android) does not have support for DTLS 1.2

✓ **Users no longer need to write their own!**

✓ Same licensing model – GPLv2 or commercial

© Copyright 2016 wolfSSL
LIGHTWEIGHT OPEN MESSAGING PROTOCOL

✓ Based on MQTT v3.1.1 specification

✓ Small size: **3.6kB**

✓ QoS Levels 0-2, support for TCP or TLS

✓ Examples and support available

✓ Used in upcoming **wolfSSL Secure Firmware Update** package

© Copyright 2016 wolfSSL
PORTABLE SCEP IMPLEMENTATION

✓ **Issuing** and **revocation** of certificates

✓ Protocol originally developed by CISCO

✓ **Lightweight, portable** SCEP implementation

✓ Uses wolfCrypt for crypto operations
PORTABLE SSH SERVER

- SSH == “Secure Shell”
- Often used for remote access, file transfer
- Uses wolfCrypt primitives under the hood
- Currently in development – Release Planned for 2016!
HARDWARE CRYPTOGRAPHY

Kinetis K60 mmCAU vs. wolfCrypt Software

© Copyright 2016 wolfSSL
Intel Crypto Support

- **AES-NI**
  - Hardware-accelerated AES available in some Intel chips
  - Typically 3-5 times faster than software AES

- **AVX1/2**
  - Accelerates SHA hash functions

- **RDRAND/RDSEED**
  - Random number generation in hardware
wolfSSL Kickstart

Time: 1 Week

- Cryptography validation
- Hardware crypto support
- Unburden your engineers from the details of cryptography
- Get your cryptography done right!

• Possible uses
  - Get wolfSSL brought up on a board!
wolfSSL is a lightweight C-language-based SSL/TLS library targeted for embedded, RTOS, or resource-constrained environments primarily because of its small size, speed, and portability. wolfSSL supports industry standards up to the current TLS 1.2 and DTLS 1.2 levels, is up to 20 times smaller than OpenSSL, offers a simple API, an OpenSSL compatibility layer, OCSP and CRL, and offers several progressive ciphers. wolfSSL is under active development, and should be chosen over yaSSL when possible.

yaSSL
yaSSL is a C++ based SSL library for embedded and RTOS environments targeted at individuals who prefer to use the C++ language. yaSSL supports industry standards up to TLS 1.1, and also includes an OpenSSL compatibility interface. CyaSSL should be chosen over yaSSL when possible.

Crypto Engines

wolfCrypt
The wolfCrypt embedded cryptography engine is a lightweight cryptography library targeted for embedded, RTOS, and resource constrained environments primarily because of its small size, speed, and portability. wolfCrypt supports the most popular algorithms and ciphers as well as progressive ones such as HC-128, RABBIT, NTRU, and SimK. wolfCrypt is stable, production-ready, and backed by an excellent support team.

wolfCrypt FIPS
The wolfCrypt software library is under testing at the leading Cryptographic Security Testing (CST) Laboratory. A FIPS 140-2 Level 1 certificate is expected to be issued in 1Q2013. For additional information, visit the wolfCrypt FIPS FAQ or contact fips@wolfssl.com

Wrappers

wolfSSL JNI
For Java applications that wish to leverage the Industry-leading wolfSSL SSL/TLS implementation for secure communication, this JNI wrapper provides an interface to give those applications support for the current SSL/TLS standards up to TLS 1.2 and DTLS 1.2.
wolfssl.com
Open Source Internet Security

Email: info@wolfssl.com
Phone: (425) 245-8247
Features

• Collect and decrypt SSL / TLS traffic

• Possible uses:
  - Analyzing Network Problems
  - Detecting network misuse by internal and external users
  - Monitoring network usage and data in motion
  - Debugging client/server communications

© Copyright 2016 wolfSSL
Features

• Enable encryption between memcache servers and clients
• Memcache + SSL = 4X faster than direct to database

Ask about our BETA version, available now!
Benchmarks:

Queries per Second

- DB cache
- AES
- RC4
- HC-128

New TLS Connections per Second

- OpenSSL RSA
- CyaSSL RSA
- CyaSSL NTRU

© Copyright 2016 wolfSSL