wolfSSL

Open Source Internet Security

Company / Product Overview
October, 2016

http://www.wolfssl.com
(425) 245-8247

ABOUT US

Founded: 2004

Location: Bozeman, MT
Seattle, WA
Portland, OR

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

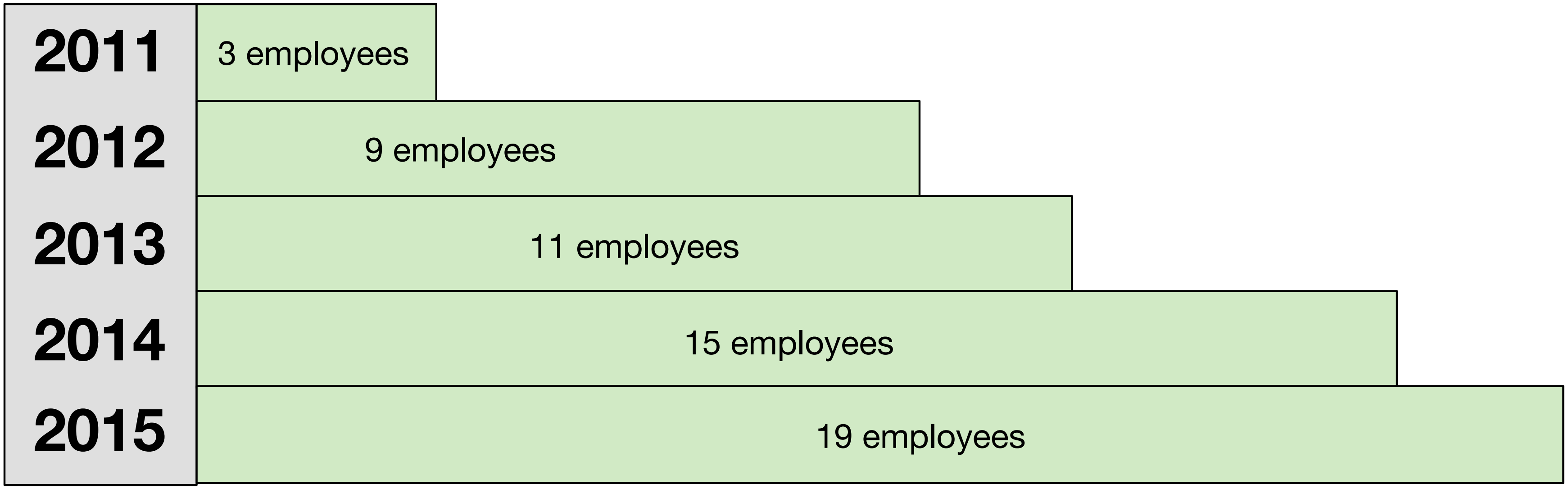
Products:
- wolfSSL
- wolfSSL FIPS
- wolfCrypt
- wolfSSH
- wolfMQTT
- wolfSCEP
- wolfSSL Inspection
- yaSSL

A GROWING COMPANY!

wolfSSL is Growing!

300 OEM Customers

15 Resale Partners



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

BROAD PARTNER PROGRAM

Industry Partnerships

ARM CONNECTED
intel Software Partner
freescale
MARVELL
TEXAS INSTRUMENTS
MICROCHIP
life.augmented
SAMSUNG
mentor embedded
Green Hills SOFTWARE
IAR SYSTEMS
NXP
RENESAS PARTNER Alliance
Atmel
ANALOG DEVICES
WIND

SECURING CONNECTIONS

Smart Home

Smart Grid

Battlefield Communication

VoIP

M2M

Cloud Services

Automotive / Smart Cars

Factory Automation

Currently Securing

2 Billion

Connections!

Internet of Things

Smart Energy

IoT

Sensors

Appliances

Connected Home

Games

Databases

Web Servers

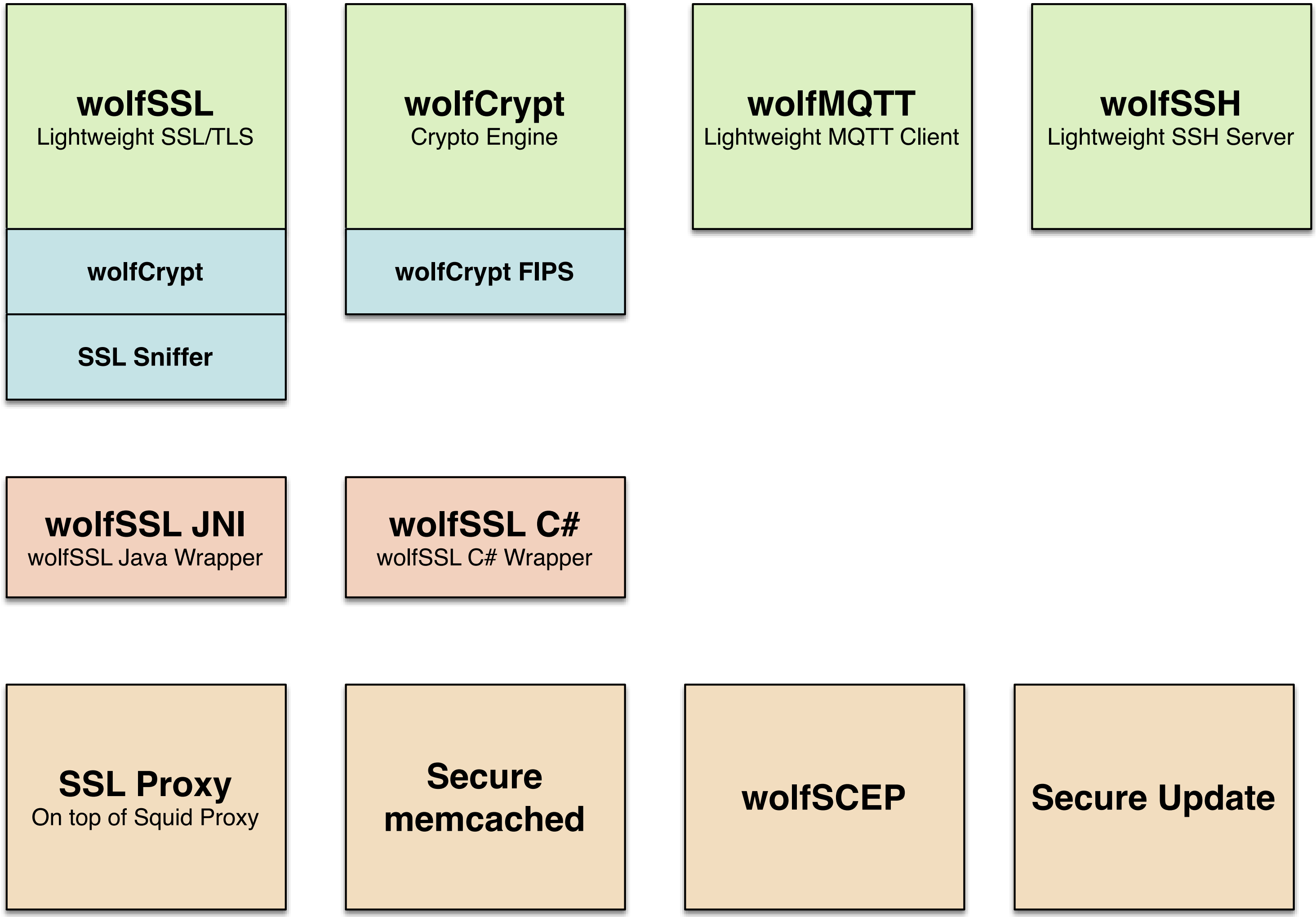
Applications

Mobile Phones

Routers

wolfSSL

WOLFSSL PRODUCTS



wolfSSL
Lightweight SSL/TLS

wolfCrypt

SSL Sniffer

wolfCrypt
Crypto Engine

wolfCrypt FIPS

wolfMQTT
Lightweight MQTT Client

wolfSSH
Lightweight SSH Server

wolfSSL JNI
wolfSSL Java Wrapper

wolfSSL C#
wolfSSL C# Wrapper

SSL Proxy
On top of Squid Proxy

Secure memcached

wolfSCEP

Secure Update

WOLFSSL PRODUCTS

wolfSSL
Lightweight SSL/TLS

wolfCrypt

SSL Sniffer

wolfCry
Crypto E

wolfMQTT
...ight MQTT Client

wolfSSH
Lightweight SSH Server

wolfSSL
wolfSSL Java Wrap

SSL Proxy
On top of Squid Proxy

memcac

...olfSCEP

Secure Update

Dual Licensed!

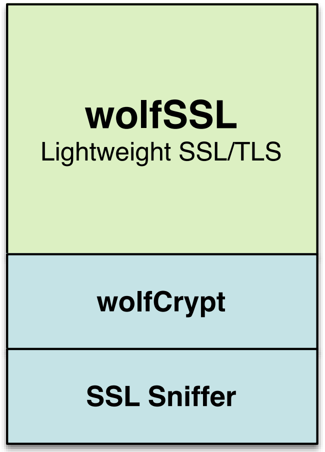
🔒 **Commercial** License	**Open Source** GPLv2 License

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)


wolfSSL
Lightweight SSL/TLS

wolfCrypt

SSL Sniffer

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, SafeRTOS, Freescale MQX, Nucleus, TinyOS, HP/UX, ARC MQX

…

WOLFSSL

Lightweight SSL / TLS Library

ADDITIONAL FEATURES:

- ✓ **OpenSSL Compatibility Layer**

OpenSSL Cryptography and SSL/TLS Toolkit

- ✓ **Web Server Integration**

NGINX LIGHTTPD fly light.

- ✓ **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**

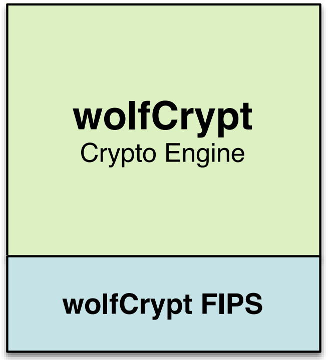
wolfSSL

WOLFCRYPT

Cryptography Library

PORTABLE MODULAR CRYPTOGRAPHY

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



wolfCrypt
Crypto Engine

wolfCrypt FIPS

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

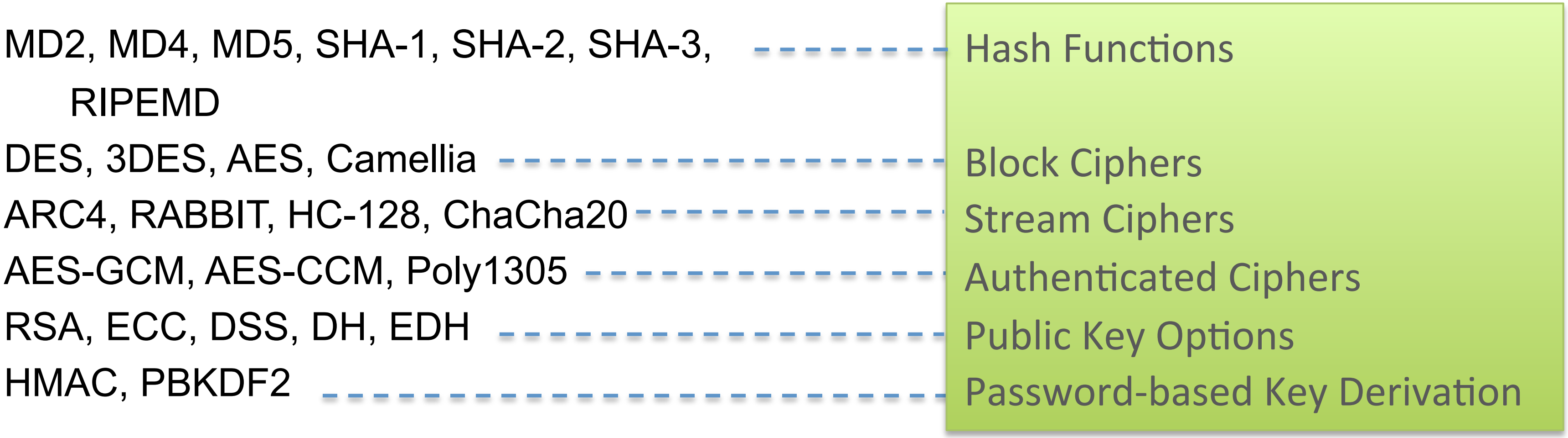
RSA, ECC, DSS, DH, EDH, NTRU
HMAC, PBKDF2, PKCS#5
ECDH-ECDSA, ECDHE-ECDSA,
ECDH-RSA, ECDHE-RSA,
Curve25519, Ed25519

…

WOLFCRYPT

Cryptography Library

Algorithms



MD2, MD4, MD5, SHA-1, SHA-2, SHA-3, RIPEMD	Hash Functions
DES, 3DES, AES, Camellia	Block Ciphers
ARC4, RABBIT, HC-128, ChaCha20	Stream Ciphers
AES-GCM, AES-CCM, Poly1305	Authenticated Ciphers
RSA, ECC, DSS, DH, EDH	Public Key Options
HMAC, PBKDF2	Password-based Key Derivation

WOLFSSL JNI

wolfSSL JNI Wrapper

BRINGING WOLFSSL TO JAVA USERS

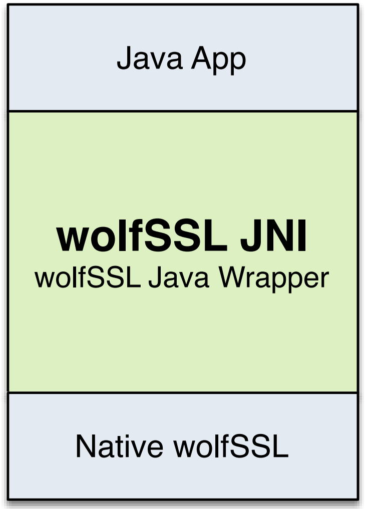
✓ **JNI wrapper** around wolfSSL

✓ 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



WOLFMQTT

MQTT Client with TLS support

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

wolfMQTT
Lightweight MQTT Client

WOLFSCEP

Simple Certificate Enrollment Protocol

PORTABLE SCEP IMPLEMENTATION

- ✓ **Issuing** and **revocation** of certificates
- ✓ Protocol originally developed by CISCO
- ✓ **Lightweight**, **portable** SCEP implementation
- ✓ Uses wolfCrypt for crypto operations

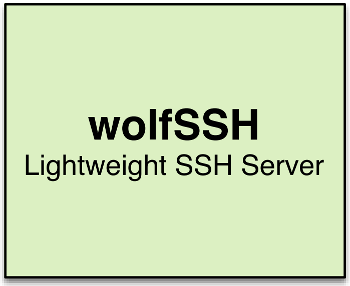
wolfSCEP

WOLFSSH

Lightweight SSH Server

PORTABLE SSH SERVER

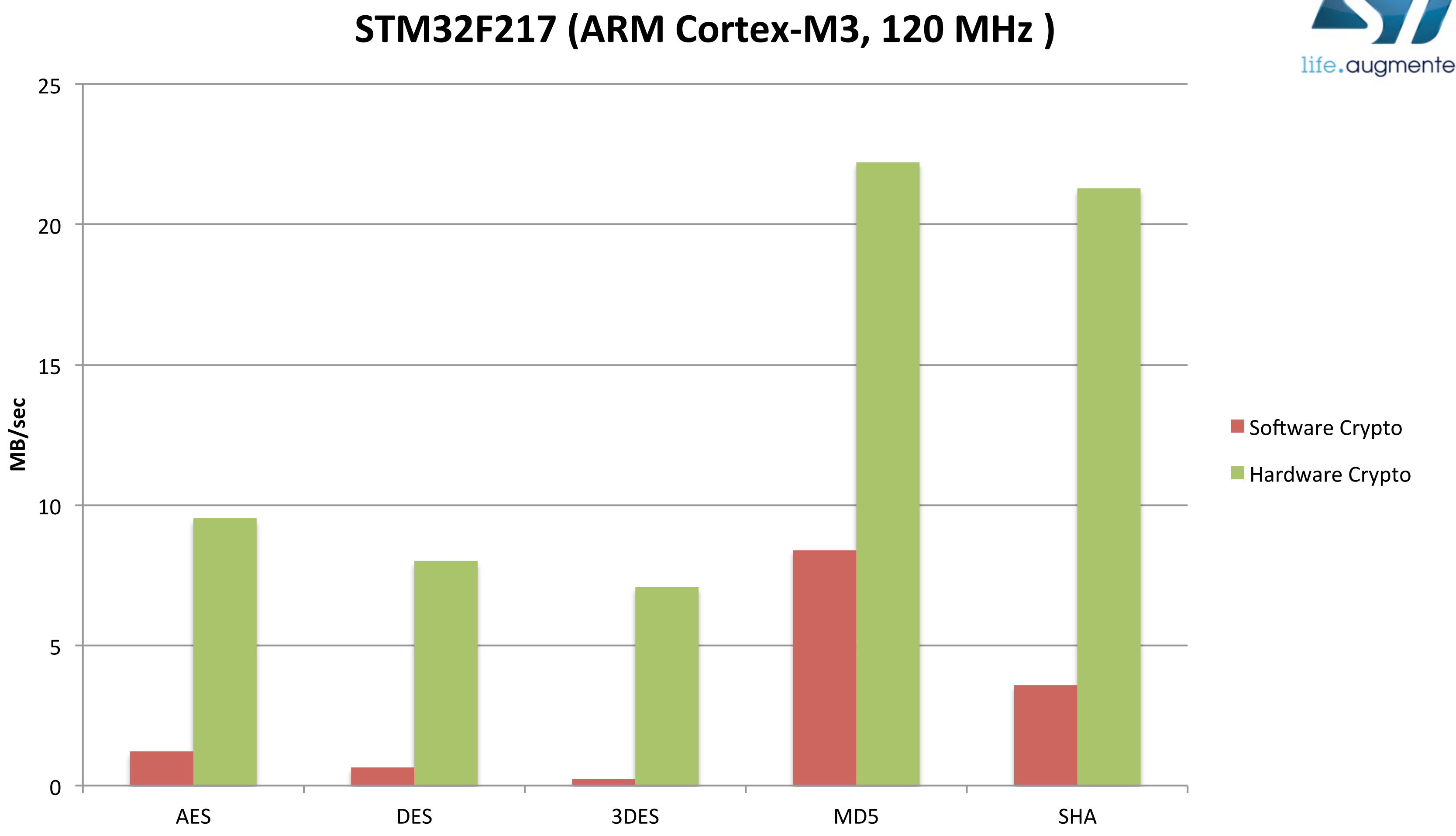
- ✓ **SSH == “Secure Shell”**
- ✓ Often used for remote access, file transfer
- ✓ Uses wolfCrypt primitives under the hood
- ✓ Currently in development – **Release Planned for 2016**!



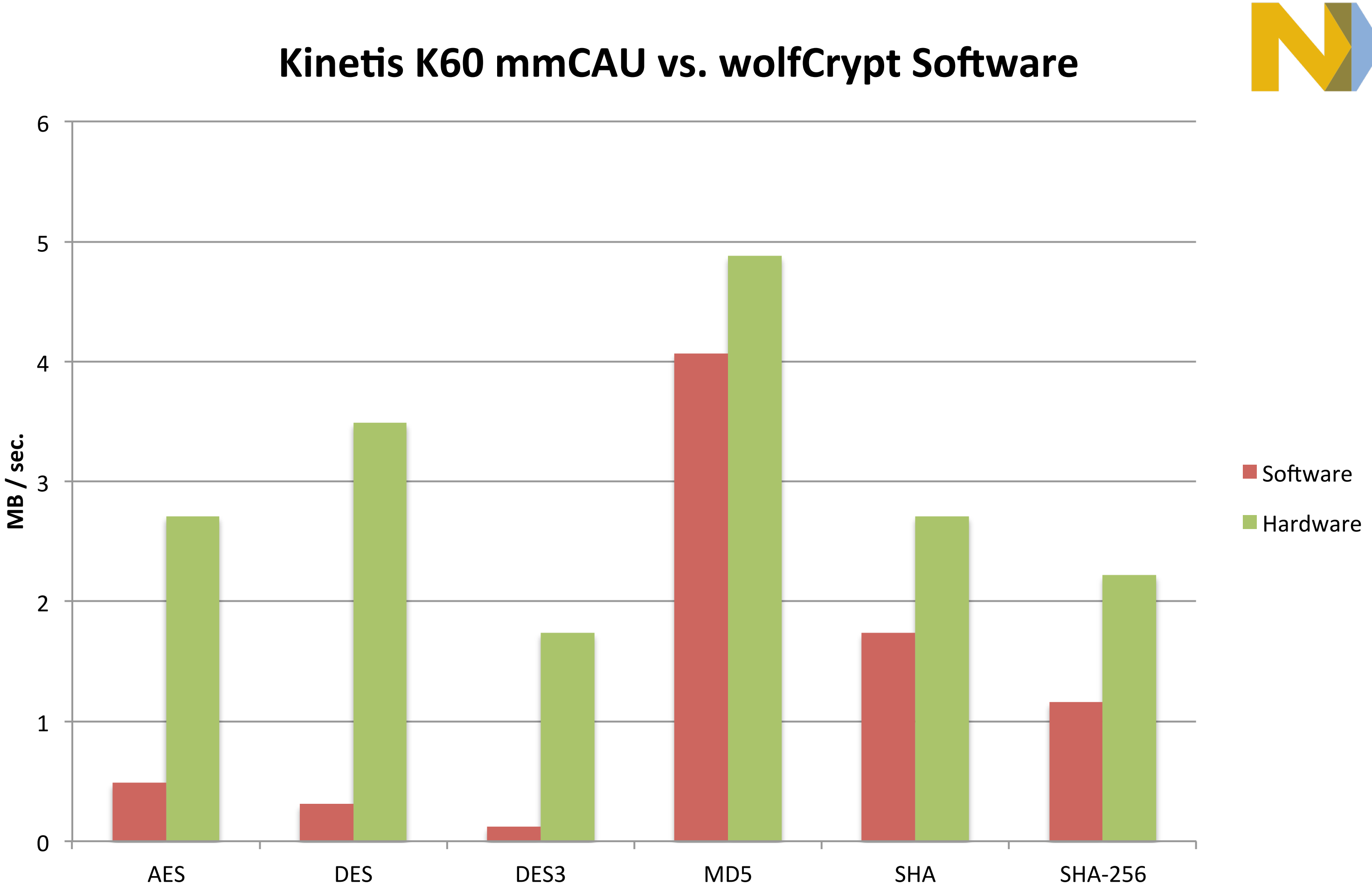
wolfSSH

Lightweight SSH Server

HARDWARE CRYPTOGRAPHY



HARDWARE CRYPTOGRAPHY



HARDWARE CRYPTOGRAPHY

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

SECURE YOUR DEVICE

wolfSSL Kickstart

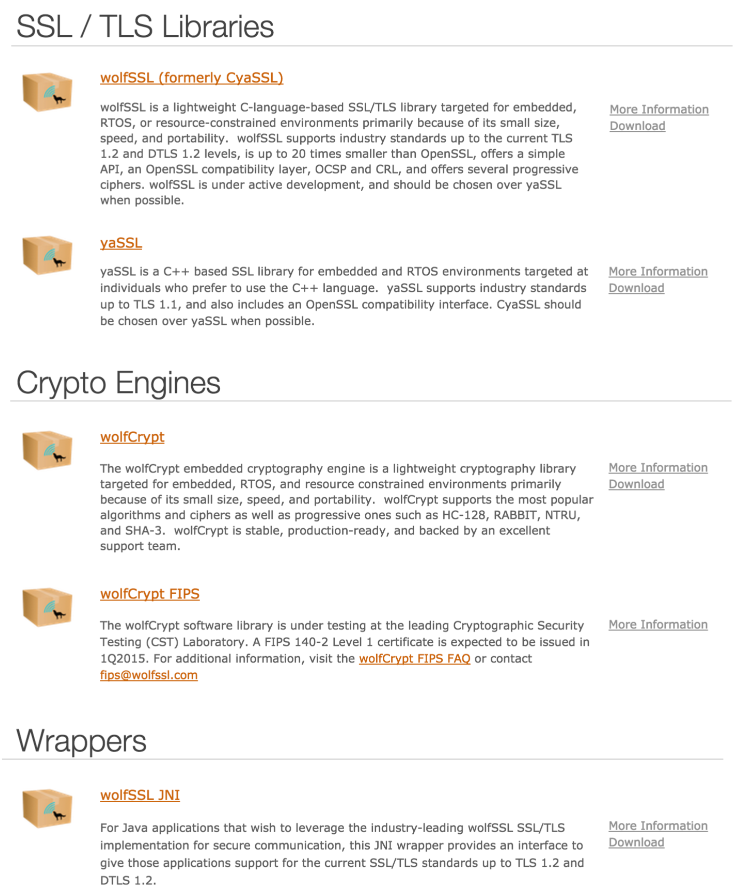
Time: **1 Week**

- 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!

DOWNLOAD WOLFSSL TODAY!

wolfssl.com



SSL / TLS Libraries

wolfSSL (formerly CyaSSL)

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.

More Information
Download

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.

More Information
Download

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 SHA-3. wolfCrypt is stable, production-ready, and backed by an excellent support team.

More Information
Download

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 1Q2015. For additional information, visit the wolfCrypt FIPS FAQ or contact fips@wolfssl.com

More Information

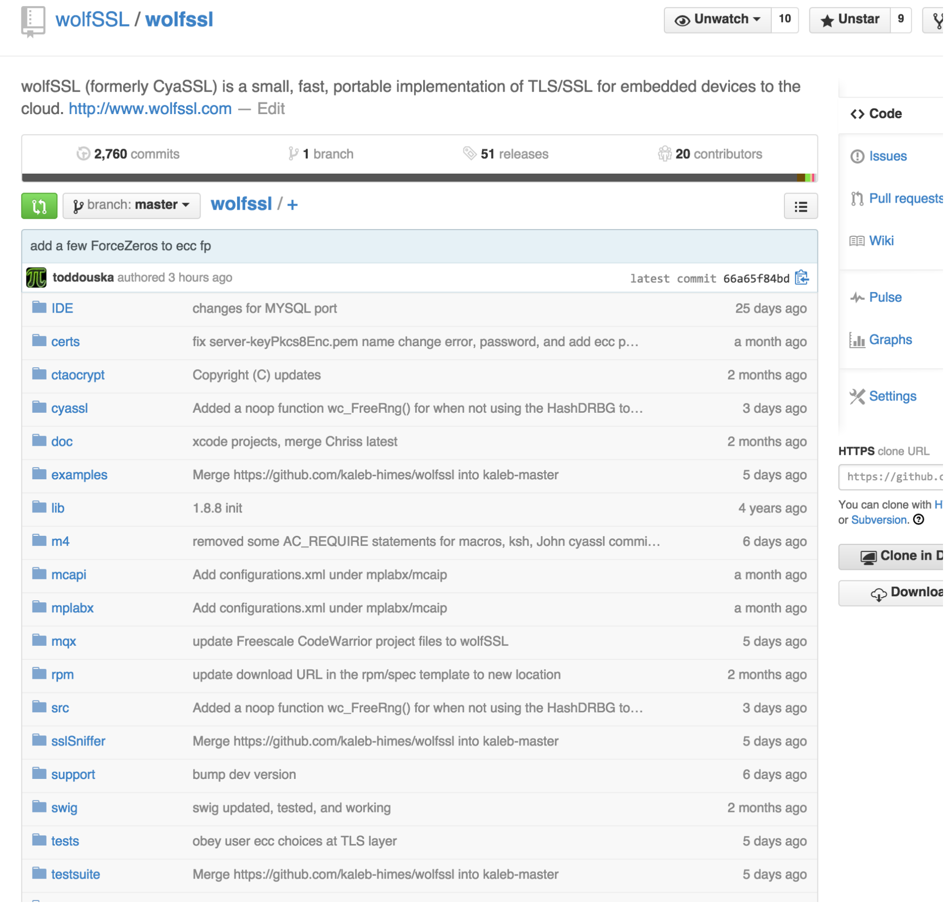
Wrappers

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.

More Information
Download

github.com



wolfSSL (formerly CyaSSL) is a small, fast, portable implementation of TLS/SSL for embedded devices to the cloud. http://www.wolfssl.com — Edit

2,760 commits | 1 branch | 51 releases | 20 contributors

branch: master | wolfssl / +

add a few ForceZeros to ecc fp

toddouska authored 3 hours ago — latest commit 66a65f84bd

IDE	changes for MYSQL port	25 days ago
certs	fix server-keyPkcs8Enc.pem name change error, password, and add ecc p…	a month ago
ctaocrypt	Copyright (C) updates	2 months ago
cyassl	Added a noop function wc_FreeRng() for when not using the HashDRBG to…	3 days ago
doc	xcode projects, merge Chriss latest	2 months ago
examples	Merge https://github.com/kaleb-himes/wolfssl into kaleb-master	5 days ago
lib	1.8.8 init	4 years ago
m4	removed some AC_REQUIRE statements for macros, ksh, John cyassl commi…	6 days ago
mcapi	Add configurations.xml under mplabx/mcaip	a month ago
mplabx	Add configurations.xml under mplabx/mcaip	a month ago
mqx	update Freescale CodeWarrior project files to wolfSSL	5 days ago
rpm	update download URL in the rpm/spec template to new location	2 months ago
src	Added a noop function wc_FreeRng() for when not using the HashDRBG to…	3 days ago
sslSniffer	Merge https://github.com/kaleb-himes/wolfssl into kaleb-master	5 days ago
support	bump dev version	6 days ago
swig	swig updated, tested, and working	2 months ago
tests	obey user ecc choices at TLS layer	5 days ago
testsuite	Merge https://github.com/kaleb-himes/wolfssl into kaleb-master	5 days ago

HTTPS clone URL
https://github.c

You can clone with H or Subversion.

LEARN MORE

wolfssl.com

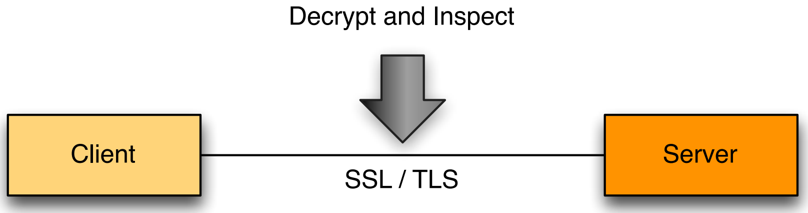
Open Source Internet Security

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

SSL INSPECTION (SSL SNIFFER)

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

SECURE MEMCACHE

Features

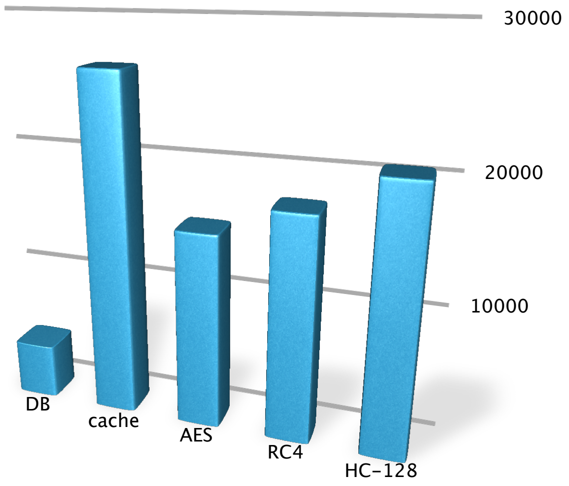
- Enable encryption between memcache servers and clients
- Memcache + SSL = 4X faster than direct to database

Ask about our BETA version, available now!

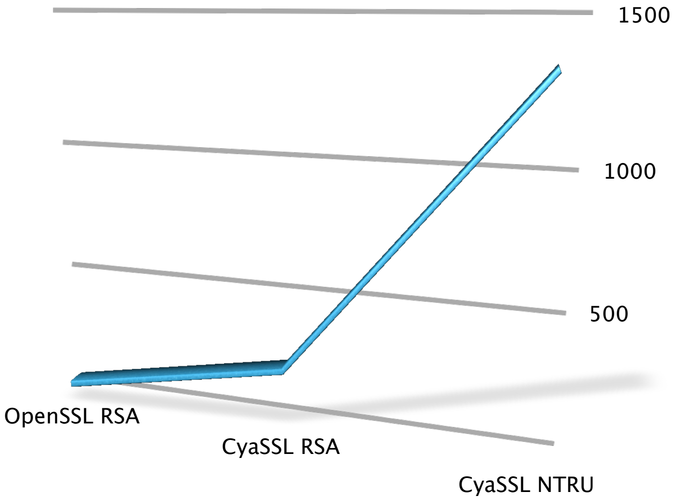
SECURE MEMCACHE

Benchmarks:

Queries per Second



New TLS Connections per Second


OpenSSL RSA
CyaSSL RSA
CyaSSL NTRU