



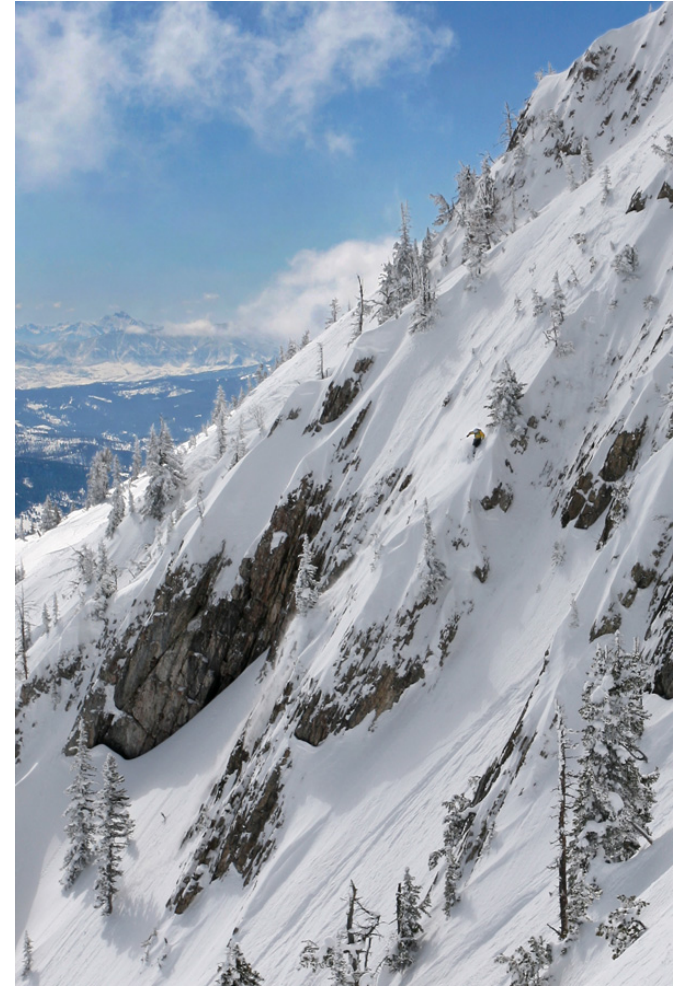
Technical / Community Update

FOSDEM 2012

About Me

Chris Conlon

Software Developer at yaSSL
Bozeman, MT

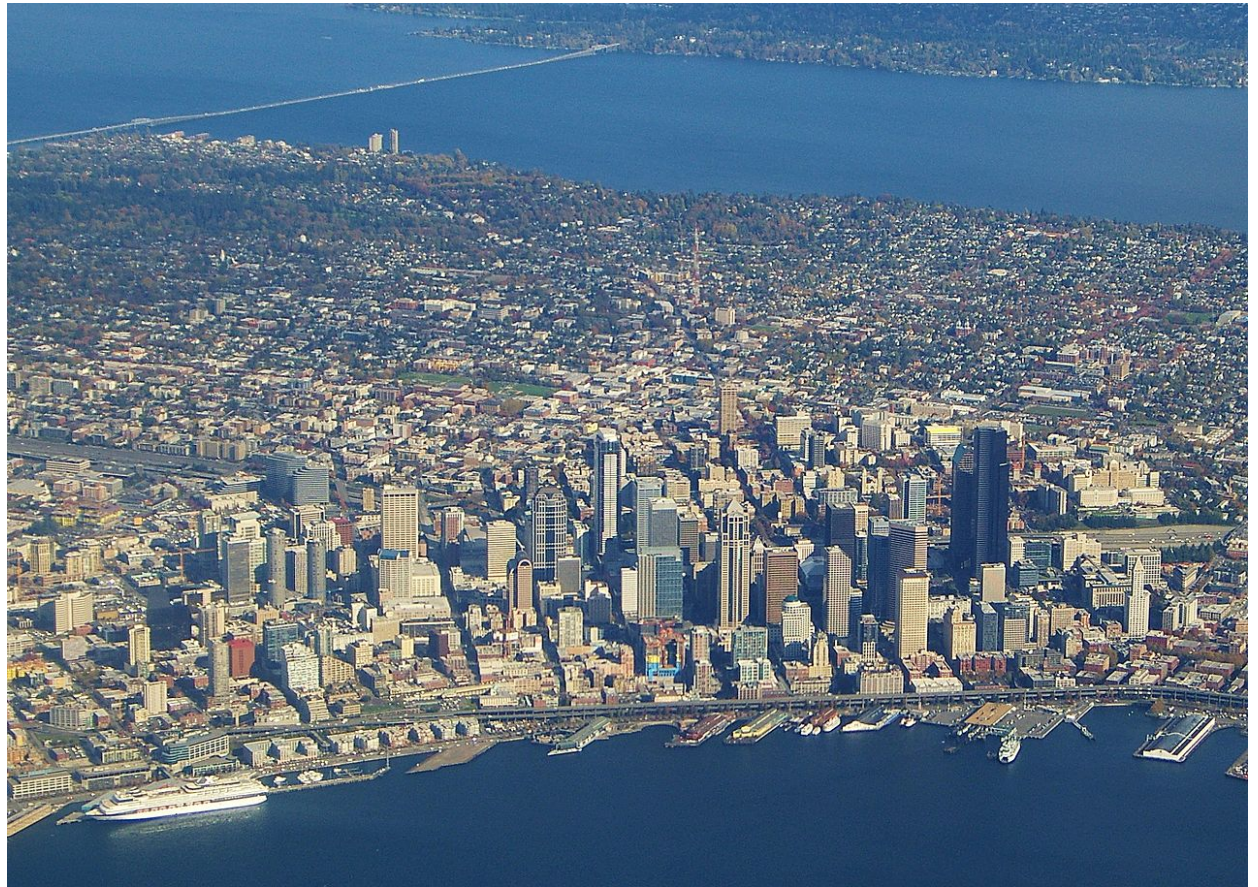


© Copyright 2012 FishEyeGuyPhotography

Who Else is Here?

Rod Weaver

Sales at yaSSL
Seattle, WA



<http://www.flickr.com/photos/84263554@N00/1698898924/>

Presentation Outline

Part I: Introduction

1. Basic Information
2. What Sets CyaSSL Apart?

Part II: Progress in 2010 - 2011

1. Technical Progress - CyaSSL
2. Technical Progress - yaSSL Embedded Web Server
3. New Ports
4. Code and Community

Part III: Wrap-Up

Part I

Introduction

Basic Information
What sets CyaSSL apart?

yet another SSL (yaSSL)



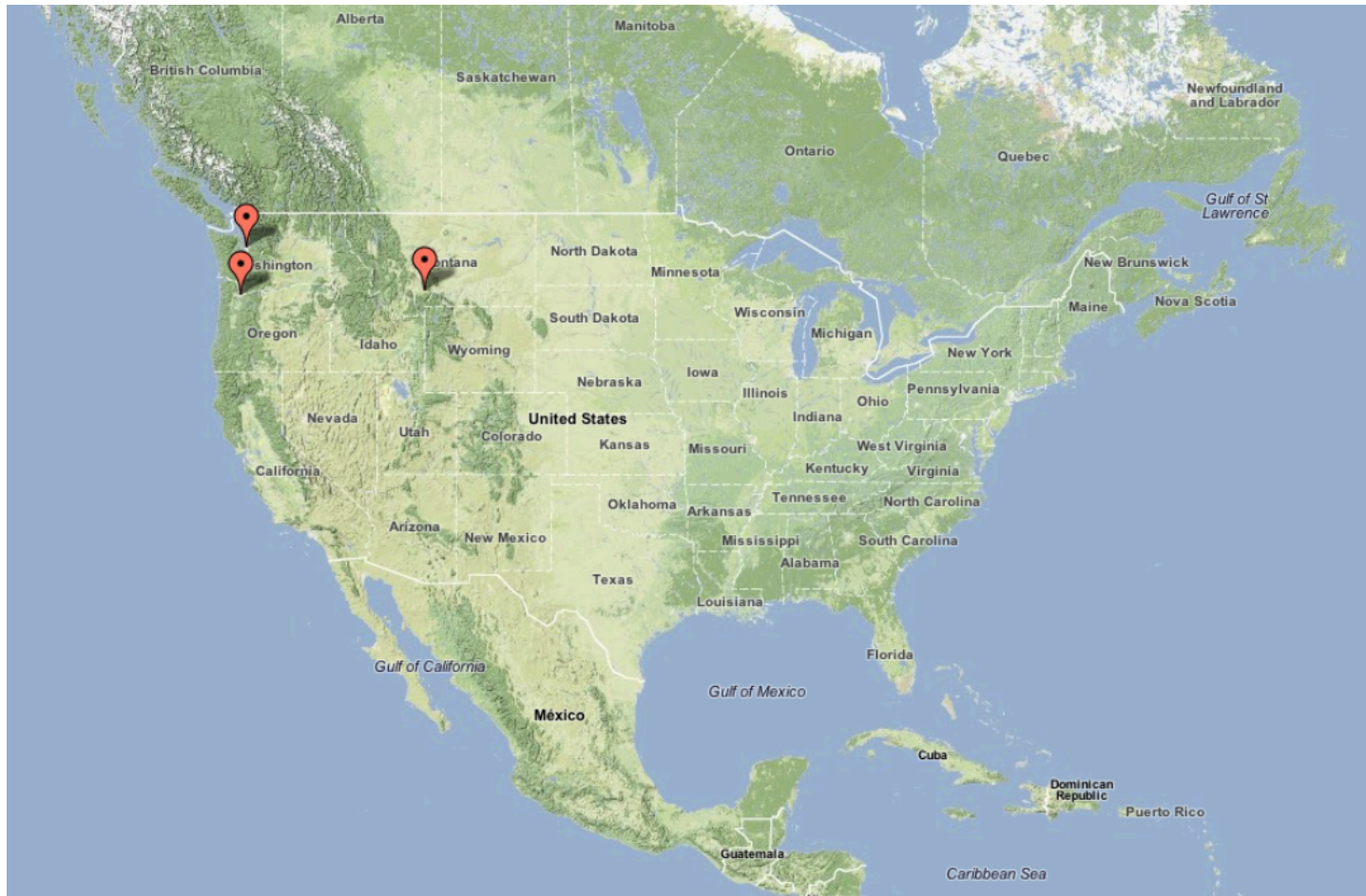
Founded: 2004

Location: Bozeman, MT
Seattle, WA
Portland, OR

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

Products: - CyaSSL, yaSSL
- yaSSL Embedded Web Server

Where in the World is yaSSL?



Where in the World is **yaSSL**?

... But used all over the world.

Current Install Base Estimations:

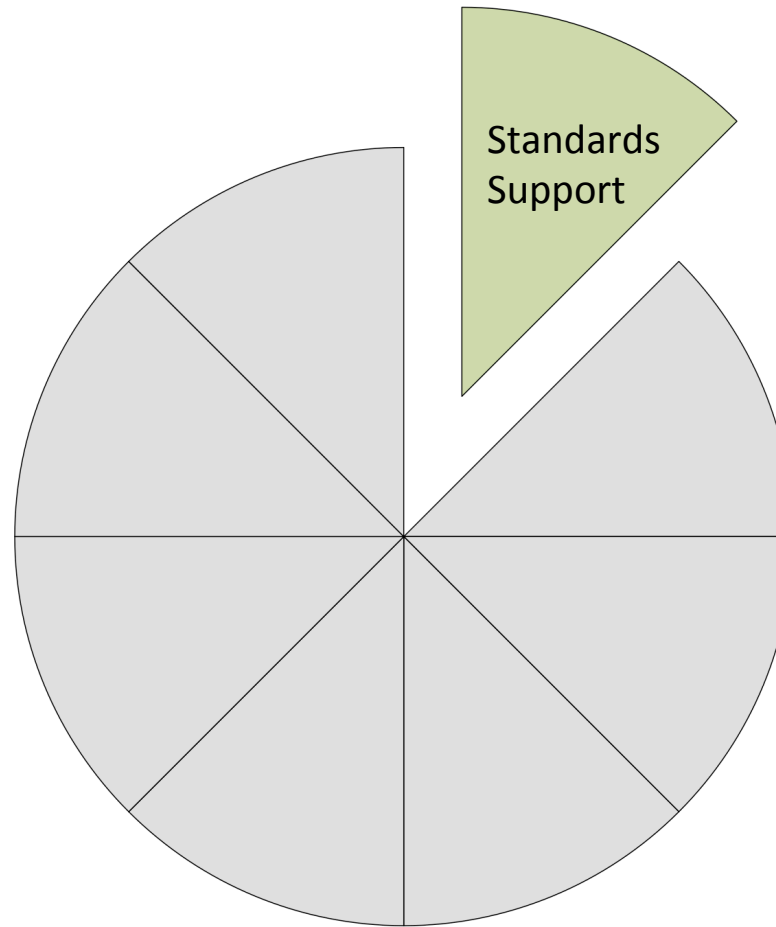
Commercially licensed distribution: **5M**

Open Source Distribution: **10-20M** units.

So, what sets CyaSSL apart?

Well...

What Sets CyaSSL Apart?



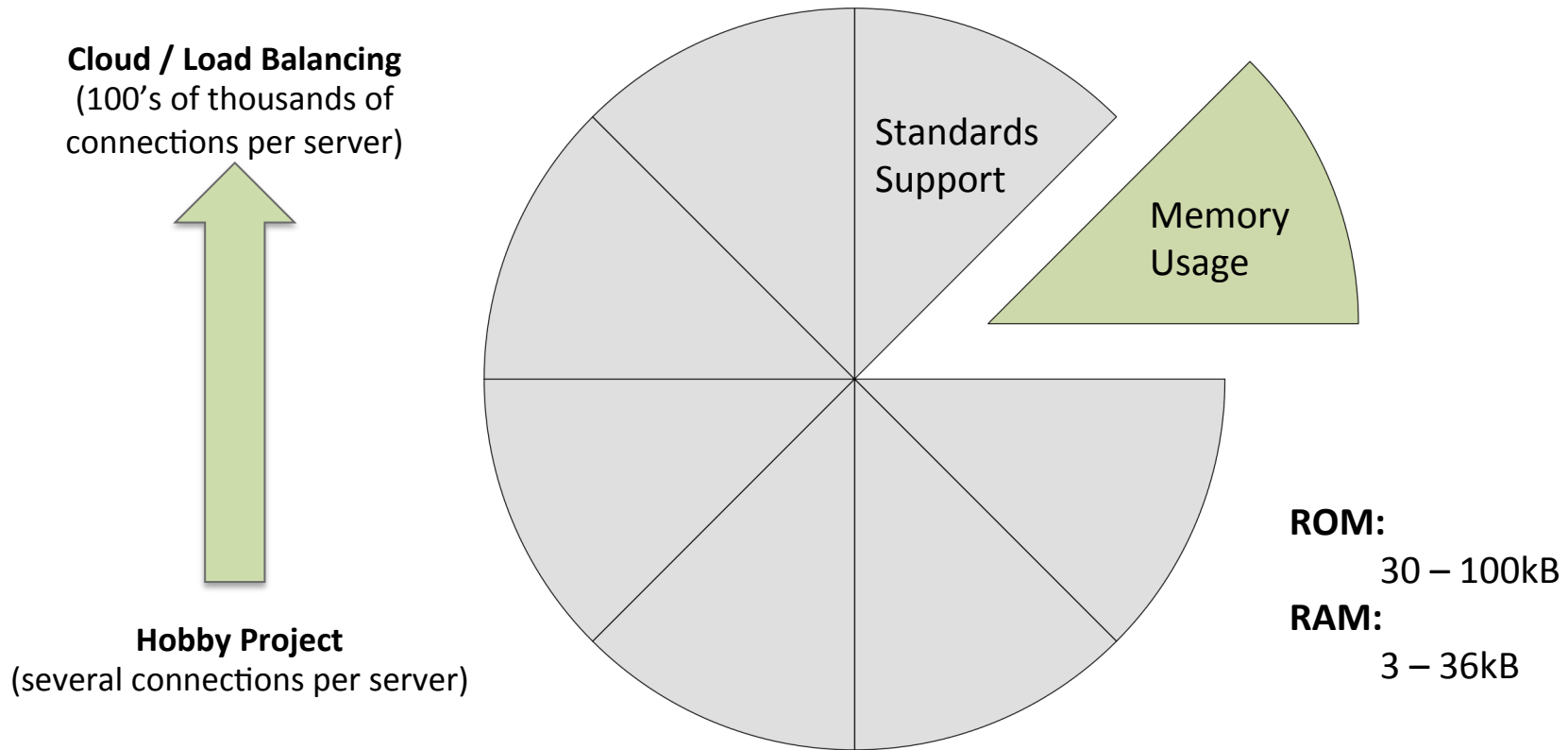
Supported Standards:

SSL 3.0

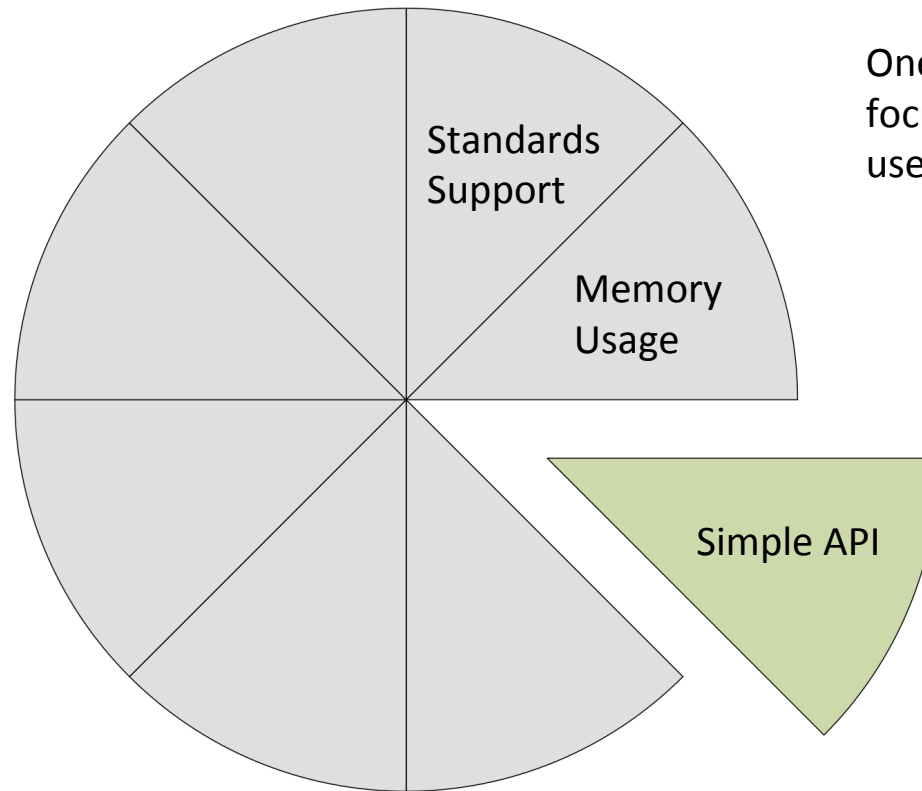
TLS 1.0, 1.1, 1.2

DTLS

What Sets CyaSSL Apart?

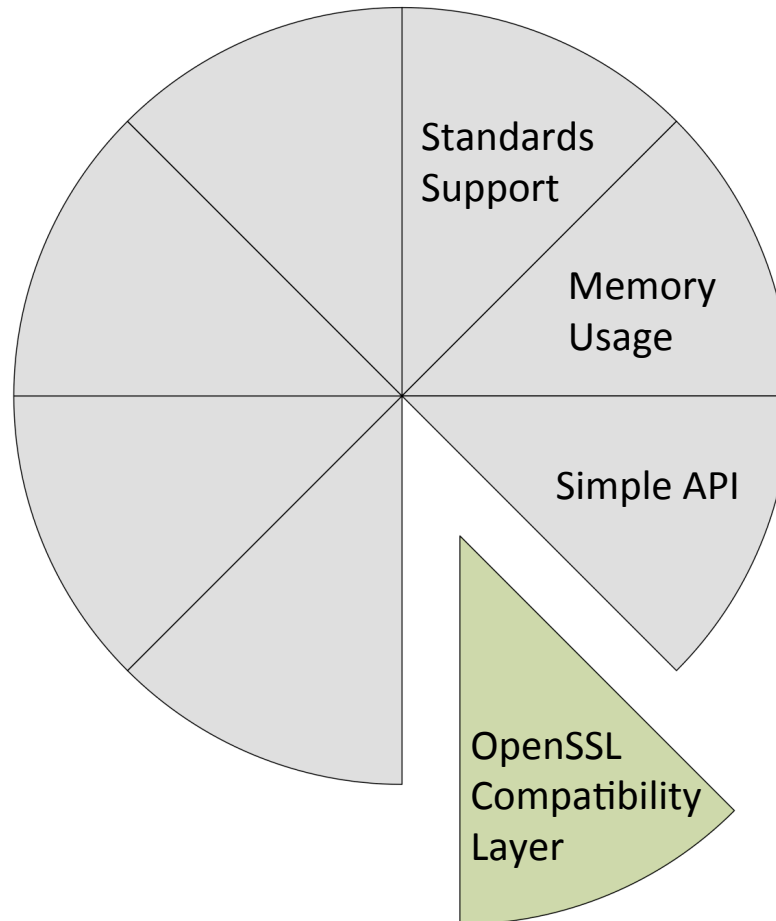


What Sets CyaSSL Apart?



One of yaSSL's key focuses is simplicity of use.

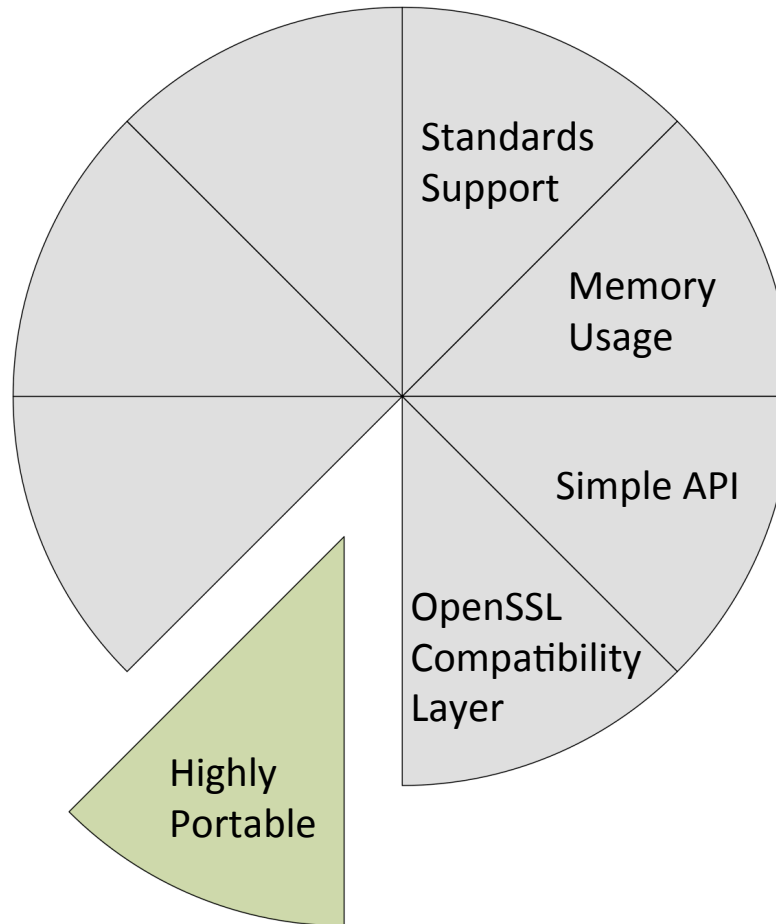
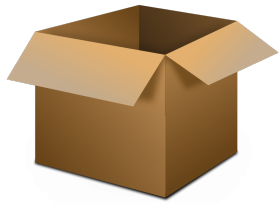
What Sets CyaSSL Apart?



Includes top 300
OpenSSL functions.

Always expanding...

What Sets CyaSSL Apart?

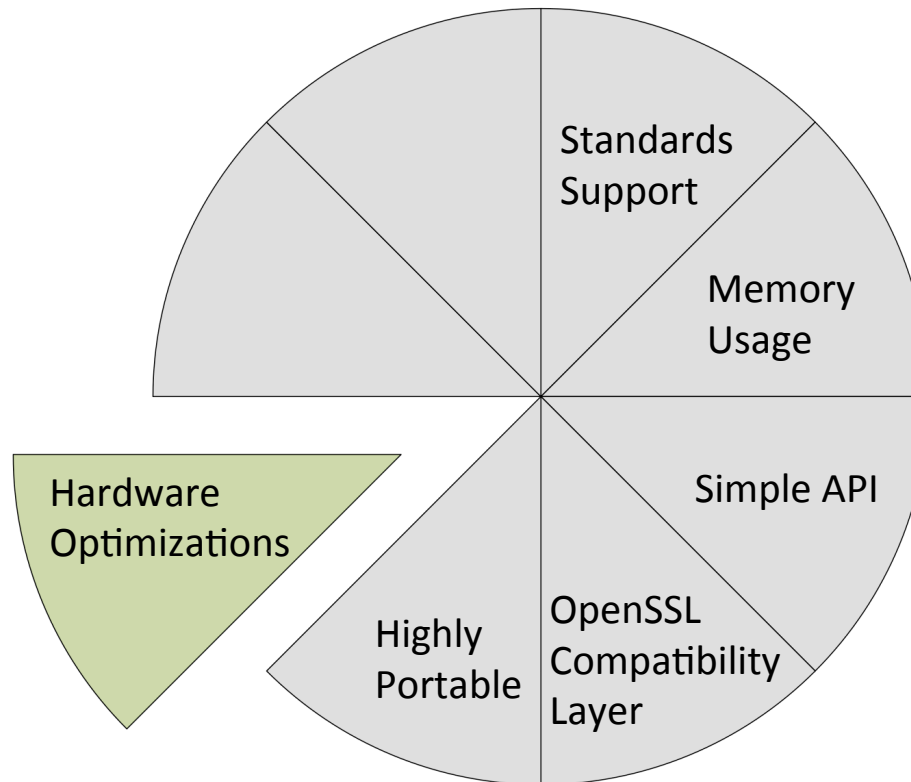
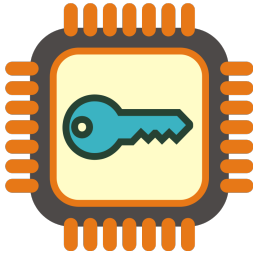


Out-of-the-box
platform support

Abstraction Layers

- OS
- Custom I/O
- Standard C lib.

What Sets CyaSSL Apart?



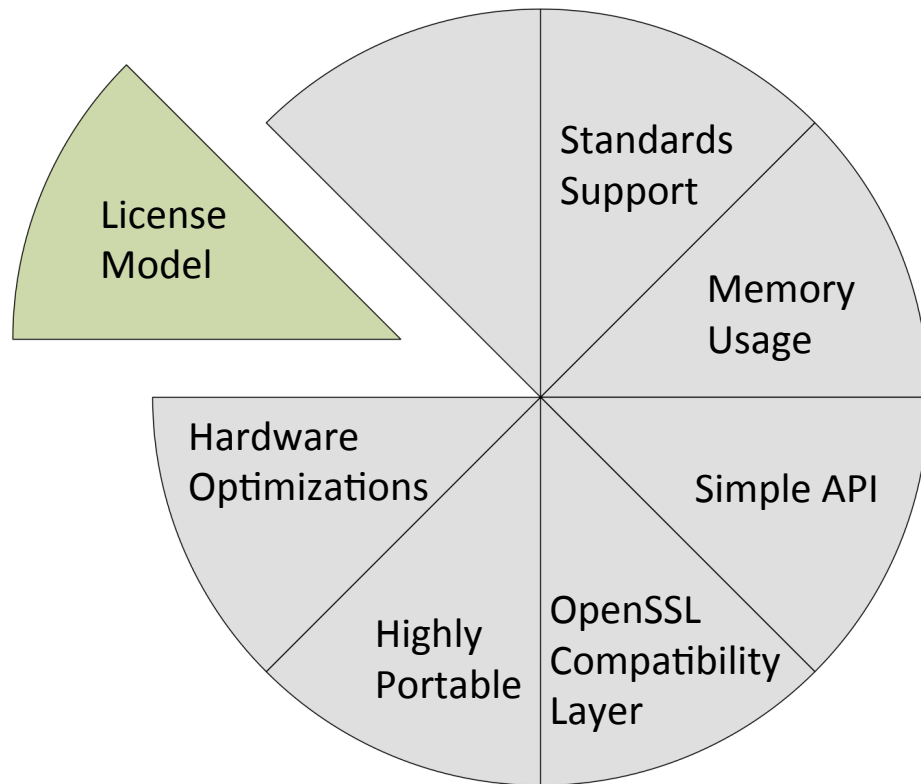
Intel AES-NI:

`--enable-aesni`

**Assembly
Optimizations:**

`--enable-fastmath`

What Sets CyaSSL Apart?



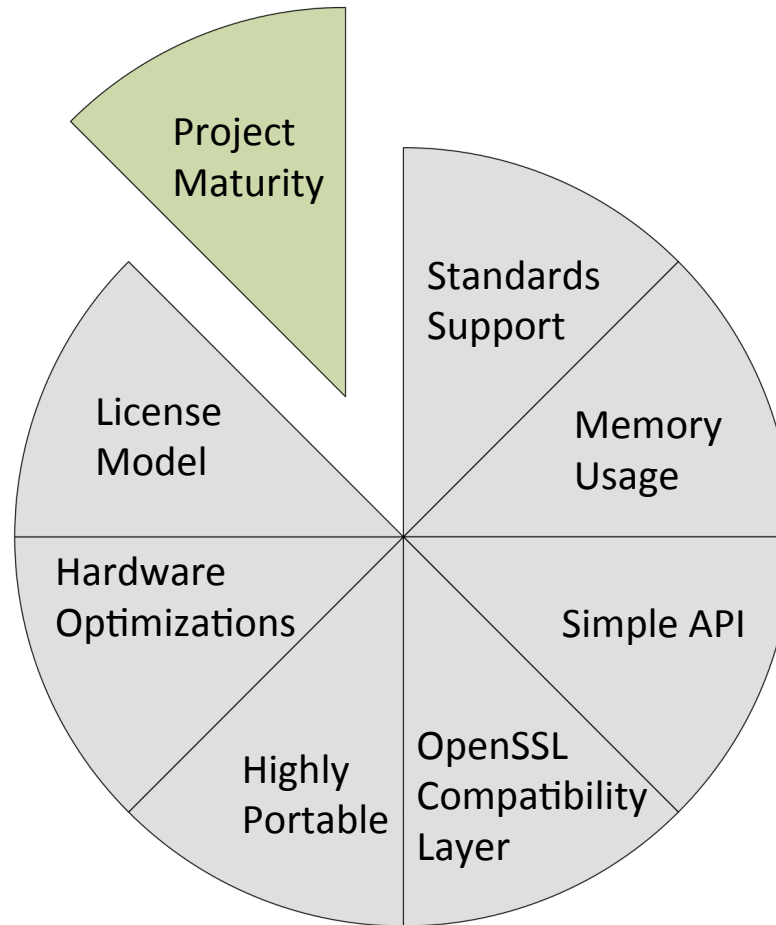
Dual Licensed:

- GPL, Commercial

Support Packages

- 3 tiers

What Sets CyaSSL Apart?



Single Code Base

Same devs since 2004
project beginning

33rd Release (2.0.6)

What Sets CyaSSL Apart?

Supported Ciphers

MD2, MD4, MD5, SHA-1, SHA-2, RIPEMD

AES, DES, 3DES, ARC4, RABBIT, HC-128

RSA, DSS, DH, EDH, NTRU

HMAC, PKCS #5 , PKCS #12 PBKDF

Hashing Functions

Block and Stream Ciphers

Public Key Options

Password-based Key Derivation

What Sets CyaSSL Apart?

Supported Operating Systems

Win32/64, Linux, Mac OS X, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded Linux, Haiku, OpenWRT, iPhone (iOS), Android, Nintendo Wii and Gamecube through DevKitPro, QNX, MontaVista, OpenCL, NonStop, Tron/itron/microitron, Micrium's μ C OS, FreeRTOS, Freescale MQX



Part II

2010 - 2011

What's happened in the past
year with yaSSL?

Technical News
New Ports

What's Happened in the Past Year?

LOTS!

... of cool stuff.

What's Happened in the Past Year?

Technical News

CyaSSL, yaSSLEWS

Technical News - CyaSSL

New Cipher Suites

- Elliptic Curve Cryptography (ECC, EC-DSA, EC-DH)

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA  
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA  
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA  
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA  
TLS_ECDHE_RSA_WITH_RC4_128_SHA  
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA  
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA  
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
```

- SHA-256

```
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256  
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256  
TLS_RSA_WITH_AES_256_CBC_SHA256  
TLS_RSA_WITH_AES_128_CBC_SHA256
```


Technical News - CyaSSL

New Cipher Suites

- NTRU suites



Technical News - CyaSSL

New Cipher Suites

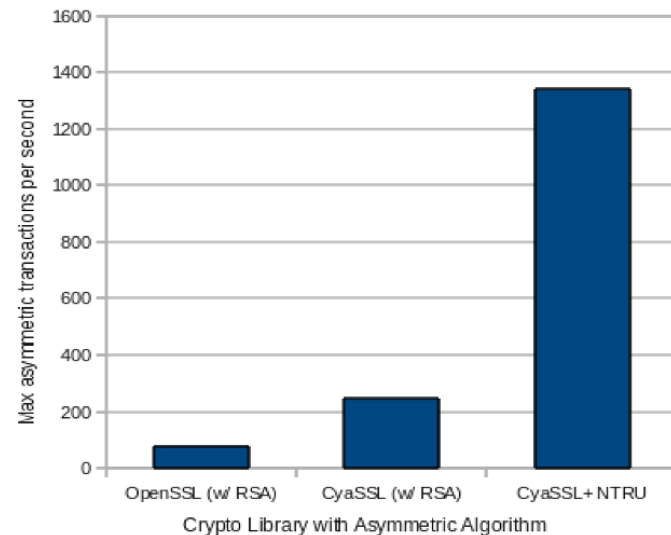
- NTRU suites

TLS_NTRU_RSA_WITH_RC4_128_SHA
TLS_NTRU_RSA_WITH_3DES_EDE_CBC_SHA
TLS_NTRU_RSA_WITH_AES_128_CBC_SHA
TLS_NTRU_RSA_WITH_AES_256_CBC_SHA

CyaSSL+NTRU is:

- **20X - 200X** faster than standard RSA
- Quantum-resistant

Performance initiating a new SSL connection
64 bit machine, 112bit security level (ie 2048bit RSA)



Technical News - CyaSSL

New Cipher Suites

- Ephemeral Diffie Hellman

Both **client** and **server** support for EDH

Technical News - CyaSSL

Other Crypto News

- AES-CTR (counter mode) support
- SHA-256 Certificate Signatures
 - Usage still very unusual
 - To stay ahead of the curve

Technical News - CyaSSL

Other Crypto News

- CTaoCrypt runtime library detection ability

Provides checks for people using public-key crypto directly in shared/dynamic library mode.



Technical News - CyaSSL

Certificate Processing

- UID parsing for X509 certificates
- Serial number retrieval
- Improved CA certificate processing
 - Parsing multiple certificates per file
 - Root certificate verification
 - X509 “CA Basic Constraint” check added

Technical News - CyaSSL

Better TLS 1.2 Support

- Comprehensive interoperability testing
- Assurance for projects migrating to TLS 1.2

Technical News - CyaSSL

Improved PKCS Support

- PKCS #8 private key encryption support

Supported Formats: PKCS #5 (v1, v2), PKCS #12 encryption

- Password-based key derivation function 2 (PBKDF2)
- PKCS #12 PBKDF

Part of our plan to get full PKCS12 support

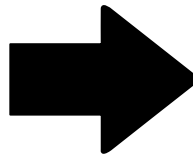
Technical News - CyaSSL

Package Design Changes

- Simplified header structure

/usr/local/cyassl

```
2
3 // old package structure
4
5 #include "ssl.h"
6 #include "aes.h"
7 #include "md5.h"
8
```



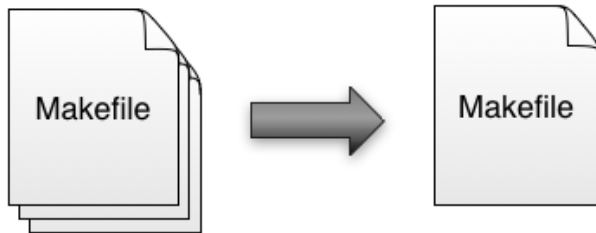
/usr/local

```
2
3 // new package structure
4
5 #include <cyassl/ssl.h>
6 #include <cyassl/ctaocrypt/aes.h>
7 #include <cyassl/ctaocrypt/md5.h>
8
```

Technical News - CyaSSL

Package Design Changes

- Single Makefile



- Compiler Visibility

Less namespace pollution

Technical News - CyaSSL

Package Design Changes

- “make test” support
 - Testsuite
 - Unit tests
 - CTaoCrypt crypto tests

Technical News - CyaSSL

Increased Portability and Customizability

- Dynamic memory runtime hooks

Ability to register memory override functions at runtime (vs compile time).

```
int CyaSSL_SetAllocators(CyaSSL_Malloc_cb malloc_function,  
                        CyaSSL_Free_cb free_function,  
                        CyaSSL_Realloc_cb realloc_function);
```

Technical News - CyaSSL

Increased Portability and Customizability

- Runtime hooks for flexible logging

Logging callback functions can be registered at runtime

```
int CyaSSL_SetLoggingCb(CyaSSL_Logging_cb log_function);
```


Technical News - yaSSL EWS

New Progress

- Released version 0.2
 - Bug fixes, feature enhancements
- Improved documentation and examples

What's Happened in the Past Year?

New Ports!

New Ports!



(<http://curl.haxx.se/>)

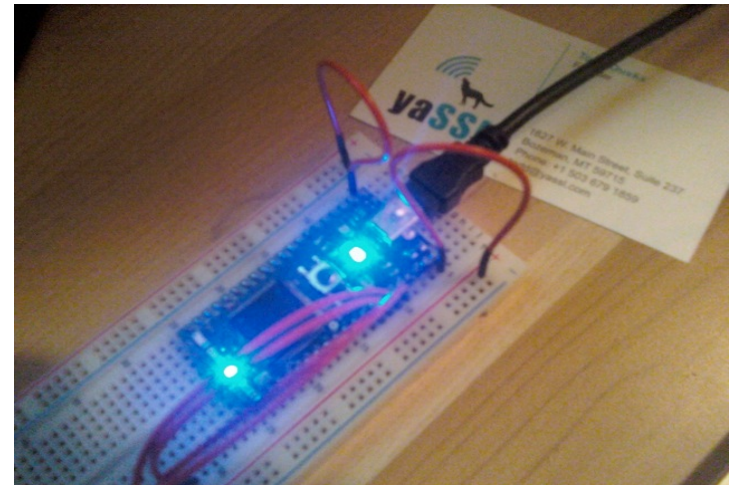
CyaSSL is now a build option

`./configure --with-cyassl --without-ssl`



(<http://www.mbed.org>)

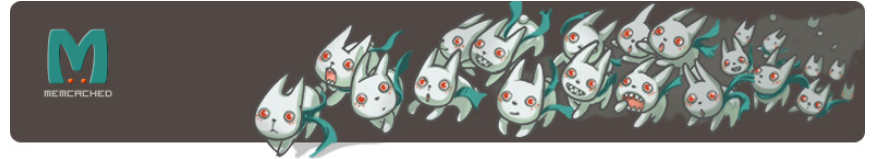
Now available for the Mbed cloud compiler!



New Ports!

memcached

(www.memcached.org)



Created a patch to add CyaSSL support ("secure memcached").

FreeRTOS, Haiku, Freescale MQX, iOS (Apple TV)

CyaSSL now supports building on these operating systems.



New Ports!

lwIP

(<https://savannah.nongnu.org/projects/lwip/>)

Lightweight TCP/IP stack
`#define CYSSL_LWIP`

Microchip PIC32

(www.microchip.com/en_US/family/32bit/)

32-bit microcontroller
`#define MICROCHIP_PIC32`



New Ports!

KLone Web Application Framework

(<http://www.koanlogic.com/klone/>)

Web application development framework,
targeted especially for embedded systems and
appliances.



OpenSSH

(<http://www.openssh.com/>)

Free SSH connectivity tool
`./configure --with-cyassl`



New Ports!

wpa_supplicant

(http://hostap.epitest.fi/wpa_supplicant/)

WPA Supplicant suitable for desktop/laptop computers and embedded systems.

`CONFIG_TLS=cyassl`

hostapd

(<http://w1.fi/hostapd/>)

User space daemon for access point and authentication servers.

`CONFIG_TLS=cyassl`

New Ports!

PPPD + EAP-TLS

(<http://ppp.samba.org/>)

(<http://www.nikhef.nl/~janjust/ppp/>)

Point-to-point protocol daemon, EAP-TLS
encapsulates the TLS messages in EAP packets.

CyaSSL EAP-TLS patch

New Ports!

*free***RADIUS**

(<http://www.freeradius.org/>)

- Most widely-deployed RADIUS server in the world.
- EAP-TLS authentication will use CyaSSL to process TLS
- CyaSSL will also perform hashing

`./configure --with-cyassl`

New Ports!

MIT Kerberos Crypto Provider

(<http://web.mit.edu/kerberos/>)

CyaSSL, NSS, OpenSSL, Built-in

```
./configure --with-crypto-impl=cyassl --with-prng-alg=os
```



New Ports!

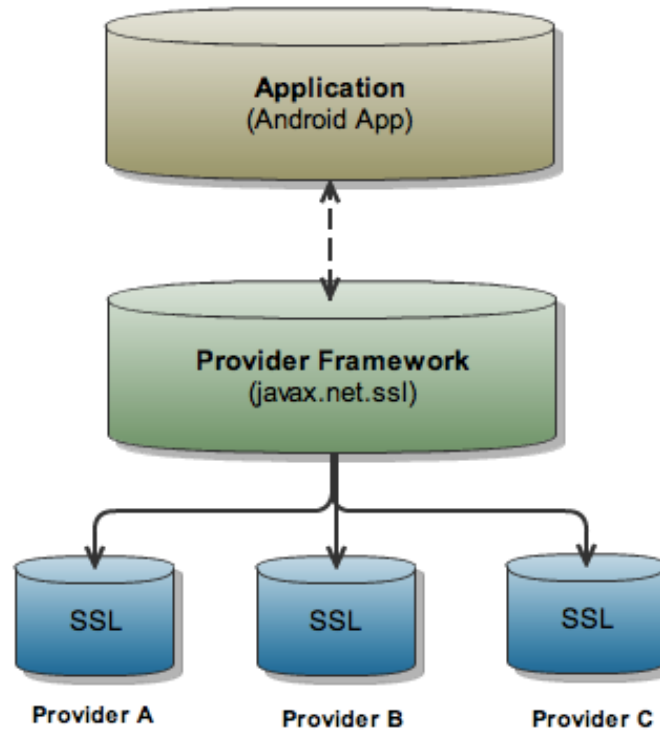
Android

Now have **3 options** for using
CyaSSL on Android



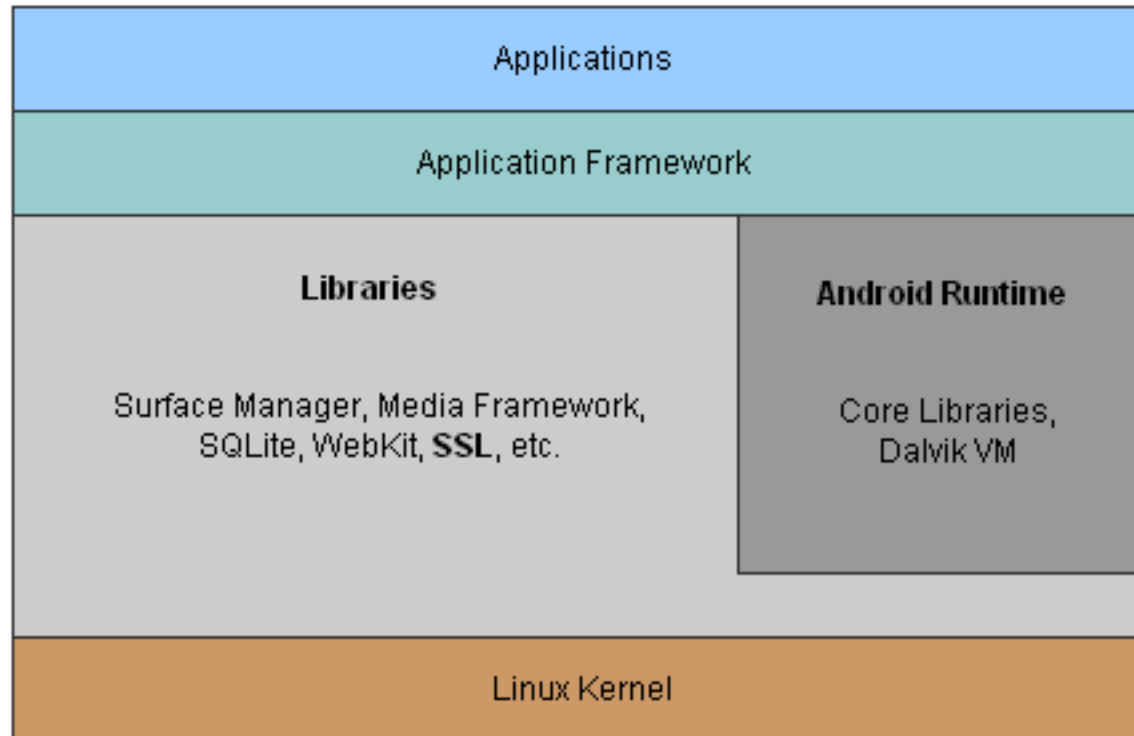
New Ports!

Android #1 : Java SSL Provider



New Ports!

Android #1 : Java SSL Provider



New Ports!

Android #2 : **CyaSSL NDK Package**

- Doesn't require users to re-build entire Android OS
- Build CyaSSL library into Android app
- Uses JNI and native NDK build system

(<https://github.com/cconlon/cyassl-android-ndk>)

New Ports!

Android #3 : Cross Compile

- Using the NDK toolchain
- Build static library (libcyassl.a) to use with NDK
- Same principle as CyaSSL NDK package, but smaller library size
- Simple to build

What's Happened in the Past Year?

Code and Community

Code and Community

GitHub

(<https://github.com/cyassl/cyassl>)

The screenshot shows the GitHub repository page for **cyassl / cyassl**. The repository is described as "CyaSSL is a small, fast, portable implementation of TLS/SSL for embedded devices to the cloud." and includes a link to www.yassl.com. The page displays various clone options (Mac, ZIP, SSH, HTTP, Git Read-Only) and a list of files with their commit history.

name	age	message	history
certs	December 28, 2011	update client-key.der to new 2048 bit one [toddouska]	
ctaocrypt	January 09, 2012	fix aes ctr cast [toddouska]	
cyassl-iphone.xcodeproj	September 25, 2011	fixes for xcode4 and cyassl2 [toddouska]	
cyassl	4 days ago	export Base64_Encode for general use [toddouska]	
doc	August 24, 2011	Brian Aker commits plus some minor changes like AM_CFLAGS getting AC_... [toddouska]	
examples	4 days ago	allow echoserver to accept 1 byte G then rest of GET for browsers wit... [toddouska]	
lib	February 05, 2011	1.8.8 init [toddouska]	
m4	August 24, 2011	Brian Aker commits plus some minor changes like AM_CFLAGS getting AC_... [toddouska]	
src	5 days ago	allow ca cache addition callback [toddouska]	
sslSniffer	September 23, 2011	change Visual Studio files to use new CyaSSL headers and layout, have... [toddouska]	

Code and Community

yaSSL Support Forums

(<http://www.yassl.com/forums>)



[Home](#) [About](#) [Products](#) [Download](#) [License](#) [Blog](#) [Docs](#) [Community](#) [Contact](#)

[Forums](#) [Search](#) [Register](#) [Login](#)



You are not logged in. Please login or register.

[Active topics](#) [Unanswered topics](#)

Welcome to the yaSSL Forums!

Please post questions or comments you have about yaSSL products here. It is helpful to be as descriptive as possible when asking your questions.

General

Forums	Topics	Posts	Last post
 Announcements Announcements to keep you up to date on what yaSSL is doing.	5	5	2011-12-07 10:17:54 by chris
 General Inquiries Topics not pertaining to a specific product	2	7	2011-01-11 10:00:03 by todd

Product Support Forums

Forums	Topics	Posts	Last post
 CyaSSL Topics relating to the CyaSSL embedded SSL library	98	272	Yesterday 15:24:25 by john
 yaSSL Topics relating to yaSSL (yet another SSL)	5	14	2011-07-27 08:43:16 by kreditas
 yaSSL Embedded Web Server Topics relating to the yaSSL Embedded Web Server	4	13	2012-01-15 01:29:40 by louis chou



Code and Community

New Partnerships



- Intel Embedded Alliance (General Member)
- KoanLogic

Wrap-Up

Thanks!

<http://www.yassl.com>

Email: info@yassl.com
chris@yassl.com

Phone: +1 206 369 4800