Technical / Community Update

FOSDEM 2012
About Me

Chris Conlon
Software Developer at yaSSL
Bozeman, MT
Who Else is Here?

Rod Weaver
Sales at yaSSL
Seattle, WA

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

© Copyright 2012 yaSSL
Where in the World is yaSSL?
Where in the World is yaSSL?

… But used all over the world.

Current Install Base Estimations:

Commerically 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?

Cloud / Load Balancing
(100’s of thousands of connections per server)

Hobby Project
(several connections per server)

Standards Support

Memory Usage

ROM:
30 – 100kB

RAM:
3 – 36kB

© Copyright 2012 yaSSL
What Sets CyaSSL Apart?

One of yaSSL’s key focuses is simplicity of use.
What Sets CyaSSL Apart?

- Standards Support
- Memory Usage
- Simple API
- Includes top 300 OpenSSL functions.
- Always expanding...
- OpenSSL Compatibility Layer

© Copyright 2012 yaSSL
What Sets CyaSSL Apart?

- Standards Support
- Memory Usage
- Simple API
- OpenSSL Compatibility Layer
- Highly Portable
- Out-of-the-box platform support
  - Abstraction Layers
    - OS
    - Custom I/O
    - Standard C lib.
What Sets CyaSSL Apart?

- Standards Support
- Memory Usage
- Simple API
- OpenSSL Compatibility Layer
- Highly Portable
- Assembly Optimizations: --enable-fastmath
- Hardware Optimizations
- Intel AES-NI: --enable-aesni
What Sets CyaSSL Apart?

Dual Licensed:
- GPL, Commercial

Support Packages
- 3 tiers

License Model

Standard Support

Memory Usage

Simple API

OpenSSL Compatibility Layer

Highly Portable

Hardware Optimizations

© Copyright 2012 yaSSL
What Sets CyaSSL Apart?

- **Single Code Base**
- Same devs since 2004 project beginning
- 33rd Release (2.0.6)

**Diagram:**
- Project Maturity
- Standards Support
- Memory Usage
- Simple API
- OpenSSL Compatibility Layer
- Highly Portable
- License Model
- Hardware Optimizations

© Copyright 2012 yaSSL
What Sets CyaSSL Apart?

Supported Ciphers

- Hashing Functions
- Block and Stream Ciphers
- Public Key Options
- Password-based Key Derivation

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
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 μC OS, FreeRTOS, Freescale MQX

© Copyright 2012 yaSSL
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
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
New Cipher Suites

- NTRU suites
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
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
Other Crypto News

- CTaoCrypt runtime library detection ability

Provides checks for people using public-key crypto directly in shared/dynamic library mode.
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
Better TLS 1.2 Support

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

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

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

• Dynamic memory runtime hooks

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

```c
int CyaSSL_SetAllocators(CyaSSL_Malloc_cb malloc_function,
                          CyaSSL_Free_cb free_function,
                          CyaSSL_Realloc_cb realloc_function);
```
Increased Portability and Customizability

• Runtime hooks for flexible logging

Logging callback functions can be registered at runtime

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

CyaSSL is now a build option
./configure --with-cyassl --without-ssl

Now available for the Mbed cloud compiler!
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 CYASSL_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!

freeRADIUS
(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
MIT Kerberos Crypto Provider
(http://web.mit.edu/kerberos/)

CyaSSL, NSS, OpenSSL, Built-in

./configure --with-crypto-impl=cyassl --with-prng-alg=os
Now have 3 options for using CyaSSL on Android
New Ports!

Android #1 : Java SSL Provider
New Ports!

Android #1: Java SSL Provider

- Applications
- Application Framework
- Libraries: Surface Manager, Media Framework, SQLite, WebKit, SSL, etc.
- Android Runtime: Core Libraries, Dalvik VM
- Linux Kernel
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

© Copyright 2012 yaSSL
What’s Happened in the Past Year?

Code and Community
GitHub
(https://github.com/cyassl/cyassl)
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

<table>
<thead>
<tr>
<th>Forums</th>
<th>Topics</th>
<th>Posts</th>
<th>Last post</th>
</tr>
</thead>
<tbody>
<tr>
<td>Announcements</td>
<td>5</td>
<td>5</td>
<td>2011-12-07 10:17:54 by chris</td>
</tr>
<tr>
<td>General Inquiries</td>
<td>2</td>
<td>7</td>
<td>2011-01-11 10:00:03 by todd</td>
</tr>
</tbody>
</table>

### Product Support Forums

<table>
<thead>
<tr>
<th>Forums</th>
<th>Topics</th>
<th>Posts</th>
<th>Last post</th>
</tr>
</thead>
<tbody>
<tr>
<td>CyaSSL</td>
<td>98</td>
<td>272</td>
<td>Yesterday 15:24:25 by john</td>
</tr>
<tr>
<td>yaSSL</td>
<td>5</td>
<td>14</td>
<td>2011-07-27 08:43:16 by kreditas</td>
</tr>
<tr>
<td>yaSSL Embedded Web Server</td>
<td>4</td>
<td>13</td>
<td>2012-01-15 01:29:40 by louis chou</td>
</tr>
</tbody>
</table>
New Partnerships

- Intel Embedded Alliance (General Member)
- KoanLogic
Wrap-Up
http://www.yassl.com

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

Phone: +1 206 369 4800

Thanks!

© Copyright 2012 yaSSL