Embedded Security for Devices

http://www.yassl.com
(206) 369-4800
1. CyaSSL Embedded SSL Library
   - Basic Information
   - What's Different?
   - Cipher Suites, Environments, TLS 1.2
   - Secure Memcache
   - Secure Firmware Updates

2. yaSSL Embedded Web Server

3. Fun yaSSL projects
   - CyaSSL on a GPU
   - CyaSSL in Use
   - Porting CyaSSL to Android
   - CyaSSL support for OpenWrt

© Copyright 2011 yaSSL
Basic Information

- Project Genesis
- C-language based SSL Library
- Targeted at embedded and RTOS environments
- Focused on size and speed optimization
- Supports all industry standards
- Highly Portable
- Dual Licensed (GPLv2 and Commercial)
- Single source base, same dev team since 2004
- Where do we fit in the SSL ecosystem?

Up to 20 times smaller than OpenSSL
What's different about CyaSSL?

- Standards up to TLS 1.2, DTLS
- Minimum size of 30-100 kB
- Runtime Memory 5-50 kB
- Simple API
- OpenSSL Compatibility Layer

- Hardware optimization, including AES-NI, various assembly packs.
Cipher suites

MD2, MD4, MD5, SHA-1, SHA-512, RIPEMD
DES, 3DES, AES, ARC4, **RABBIT, HC-128**
RSA, DSS, DH **NTRU**
HMAC, PBKDF2

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

Or add your own!
CyaSSL Embedded SSL Library

Supported Environments:

- Works **without** an OS
- Works **with** an OS
- Portability is a priority for us

Win32/64, Linux, Mac OS X, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, OpenWRT, iPhone (iOS), Nintendo Wii and Gamecube through DevKitPro, QNX, MontaVista, OpenCL, NonStop, Tron/itron/microitron

© Copyright 2011 yaSSL
All Logos represented above are copyright of their respective owners.
CyaSSL Embedded SSL Library

TLS 1.2 Support

- Enhanced Security
- Less susceptible to MITM attacks
- One of the first SSL libraries to support TLS 1.2
  CyaSSL, GnuTLS

- Other TLS 1.2 firsts:
  Browser: Opera
Secure Memcache
Secure Memcache - Performance
Upcoming Project: Secure Firmware Updates

- Digitally signing firmware is a top priority today
- Protect against unauthorized updates
- Enable files to be securely loaded onto your device
- Ensure against malicious files

Code sign your updates!
CyaSSL Embedded SSL Library

- RSA Key Generation
- x509v3 Signed Certificate Generation

Make your own keys and be your own certificate authority...for all the right reasons.
yaSSL Embedded Web Server

What is it?

- Based on the Mongoose Embedded Web Server
- Uses CyaSSL for SSL functionality built-in!
- Small size
- Based on customer needs
yaSSL Embedded Web Server

Features

- HTTPS Support via CyaSSL
- Default size, with SSL enabled of less than 100 kB; 40kB without
- CGI, SSL, SSI, Resumed Downloads, Aliases and more!
- IP-based Access Control Lists
- GET, POST, HEAD, PUT, DELETE methods

Perfect for Embedded Environments
yaSSL Embedded Web Server

Supported Environments

ThreadX, VxWorks, QNX, OpenWRT, Tron, iTron, Microitron, OpenCL, MontaVista, Mac OS, Linux

License

GPL and Commercial

© Copyright 2011 yaSSL
CyaSSL on a GPU!

- Run your SSL on a GPU for performance gains
- Porting to OpenCL
- Harness latent GPU power for crypto

Image Copyright © 2011 NVIDIA Corporation
CyaSSL in Use!

Some examples of how CyaSSL Embedded SSL is being used

- Zigbee devices connecting to the cloud
- Radios in forklifts
- Printers
- Sensors
- Telepharmacy
- IP Telephony
- Super cool video games

© Copyright 2011 yaSSL
Porting **CyaSSL** to Android

- Java SSL Provider (CyaSSL)
- Can be installed alongside existing provider

© Copyright 2011 yaSSL
CyaSSL support for OpenWrt
Thanks!

http://www.yassl.com

Email: info@yassl.com
Phone: (206) 369-4800

© Copyright 2011 yaSSL