ssl/tls library usage

OpenSsl Library

-Include library headers

```
/* OpenSSL headers */
#include <openssl/bio.h>
#include <openssl/ssl.h>
#include <openssl/err.h>
```

-Compile with library flags: -lssl -lcrypto

Library Initialization

- SSL_library_init()
  - Initialize and register the available SSL/TLS ciphers and digests
- SSL_load_error_strings()
  - Use for readable error messages
- OpenSSL_add_all_algorithms()
  - Add all algorithms to the table of digests and ciphers

Library Cleanup

- SSL_shutdown()
- SSL_free()
- SSL_CTX_free()

SSL_METHOD

- Set protocol versions SSLv1, SSLv2 and TLSv1

```
SSL_METHOD* meth = SSLv23_client_method()
// many other ones available
```

SSL_CTX

- SSL connection context
- Store context information, such as keying material
- Reused for all connections

```
SSL_CTX* ctx = SSL_CTX_new(meth);
```

Startup Steps

- Initialize library
  - SSL_library_init()
  - SSL_load_error_string()
- Select SSL version
  - E.g., method = SSLv23_method()
- Get context
  - ctx= SSL_CTX_new(method)

SSL_new()

- Create a new SSL structure
- Inherit the settings of the given context

```
SSL* ssl = SSL_new(ctx);
```

SSL_set_fd()

- Associate the SSL object with a file descriptor

  int SSL_set_fd(SSL *ssl, int fd);

SSL Connection (1/2)

- Initiate the TLS/SSL handshake with a server
  - int SSL_connect(SSL *ssl)
- Get server certificate and verify it
  - SSL_get_peer_certificate(ssl)
  - SSL_CTX_set_verify(ctx, SSL_VERIFY_PEER, NULL);

SSL Connection (2/2)

- Read and write bytes to SSL connection
  - int SSL_write(SSL *ssl, const void *buf, int num)
  - int SSL_read(SSL *ssl, void *buf, int num)
- Shutdown cleanup
  - Cleanup TCP connection
  - int SSL_shutdown(SSL *ssl)
  - SSL_free(ssl)

***