Communication and Security Infrastructure, Spring 2023,

assignments list # 2 – OpenSSL (part 2), 2023-10-04

1. [**4 pts**] [**OpenSSL Cryptography**] Learn how to link against OpenSSL cryptographic library in your system/environment. In some contexts it is extremely simple, in some it requires some configuration.

   Write a simple C++ program that uses OpenSSL cryptographic interfaces to compute multiple cryptographic hashes of a selected file (use different supported hash functions, e.g. Blake2b, Blake2s, MD5, SHA1, SHA256, SHA3...)

2. [**7 pts**] [**OpenSSL TLS Context (client)**] Write a very simple, terminal-based ”web browser” (think `curl`) that supports HTTPS, that is given an `https://` address, uses OpenSSL to wrap socket in a SSL client context and presents the response to the user.

   Very basic, minimal HTTP support is required (at least for requests); for response you may simply print the HTTP headers along with the response body.

   Example:

   ```
   user@host:~$ mycurl https://cs.pwr.edu.pl/slowik
   HTTP/1.1 301 Moved Permanently
   Date: Wed, 04 Oct 2023 06:28:56 GMT
   Server: Apache/2.4.38 (Debian)
   Location: https://cs.pwr.edu.pl/slowik/
   Content-Length: 317
   Content-Type: text/html; charset=iso-8859-1

   <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
   <html><head>
   <title>301 Moved Permanently</title>
   </head><body>
   <h1>Moved Permanently</h1>
   <p>The document has moved <a href="https://cs.pwr.edu.pl/slowik/">here</a>.</p>
   <hr>
   <address>Apache/2.4.38 (Debian) Server at cs.pwr.edu.pl Port 443</address>
   </body></html>
   ```

   Note: use OpenSSL directly, not via a ready-to-use wrapper like Python’s `ssl` module.

3. [**9 pts**] [**OpenSSL TLS Context (server)**] Write a very simple HTTP server that supports HTTPS. It should simply serve files from a given directory and respond to both HTTP and HTTPS requests. A very primitive support for the HTTP protocol is sufficient.

Helpful resouorces:

1. https://github.com/openssl/openssl, esp. demos/sslecho
2. https://developer.mozilla.org/en-US/docs/Web/HTTP

/-/ Marcin Słowik