ECE 646 Cryptography and Computer Network Security

Fall 2015

Overview and Comparison of

Open Source Cryptographic Libraries

Project Specification

Members:

Cong Chen

Yuqi Wang

1 Introduction and motivation

Today is the time of data. It is vital to ensure the security of data in transit and at rest. For example, it is deadly to companies if their data was leaked or intercepted by intruders. Cryptography is a primary method to protect against such threats. There are lots of open source libraries based on different kind of languages, with their own advantages and disadvantages. Choosing a proper library is hard, especially for newcomers.

1) In this project, we will investigate basic features of multiple cryptographic libraries.
2) We will also study the differences among the selected libraries in terms of performance.
3) Another purpose of the project is to make searching easier. The project will apply Microsoft Access database to store the most important features of all investigated libraries, which will help new users to choose a library that best matches their needs.

2 Libraries to be studied

1) Cryptlib
2) NaCl
3) GNU Crypto
4) MatrixSSL
5) Mozilla NSS
6) OpenCKD
7) OpenPGPSDK
8) WolfCrypt.

3 Evaluation criteria

1) Basic information
   a) Licenses
      Different libraries use different licenses. Users always care about whether the libraries are free for their intended use or not.
   b) Documentation and ease of use
      For new users, the ease of finding documentation and learning to use certain library features really matters.
   c) Supported compilers
      One of basic criteria to be taken into consideration at the very beginning.
   d) Support for cryptographic algorithms
      Including the algorithms in public key cryptosystems, secret key cryptosystems, and key management.
   e) Key sizes
      Key sizes vary in different situations and algorithms. Collecting them makes it easier for users to choose libraries.
   f) Programming language

The programming languages supported are also key measures in choosing libraries.

g) Target microprocessors and microcontrollers.

2) Advanced features
   a) Known weaknesses and attacks
   b) Support for random key generation

3) Performance of Primitive Cryptographic Operations
   a) Speed
   b) Memory requirements.

4 Procedure

1) Reading papers and materials online.
2) Using data already existing in the SUPERCOP-eBACs database to compare performance of libraries.
3) Run the libraries on the computer and compare their performance.
4) Summarize the results in tables.
5) Use Microsoft Access to store the results.

5 Time schedule

	Date	Task description
1	Oct 17th	Final project specification.
2	Oct 18th – 31st	Study the libraries and write an overview.
3	Nov 1st – 28th	Evaluate the features.
4	Nov 29th – Dec 11th	Finish the report.
5	Dec 12th	Initial version of the report.
6	Dec 12th – 17th	Prepare for the presentation.
7	Dec 18th	Presentation.
8	Dec 19th	Final version of the report.

6 Tentative table of contents

1) Introduction.
2) Overview of libraries
3) Comparison
   a) Basic information
   b) Advanced features
   c) Performance of Primitive Cryptographic Operations
4) Conclusions
5) Possible Improvements

6) References

7 References

[1] C. Marshall, R. S. Naffah.(2003, Nov.9). Programming with GNU Crypto. [Online]. Available: http://www.gnu.org/software/gnu-crypto/manual/gnu-crypto.pdf Accessed: Oct 17 2015

[2] P. Gutmann. (2014, Apr.). Cryptlib Security Toolkit Version 3.4.2. [Online]. Available: ftp://ftp.franken.de/pub/crypt/cryptlib/manual.pdf Accessed: Oct 17 2015

[3] wolfSSL. (n.d.). *Wikipedia*. Available: https://en.wikipedia.org/wiki/WolfSSL Accessed: Oct 17 2015

[4] wolfSSL User Manual. (2015, Mar. 18). wolfSSL Inc. [Online]. Available: https://www.wolfssl.com/documentation/wolfSSL-Manual.pdf Accessed: Oct 17 2015

[5] D. J. Bernstein, T. Lange, P. Schwabe. (n.d.). The security impact of a new cryptographic library.[Online]. Available: http://cr.yp.to/highspeed/coolnacl-20120725.pdf Accessed: Oct 17 2015

[6] Diffie–Hellman key exchange. (n.d.). *Wikipedia*. Available: https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange Accessed: Oct 17 2015

[7] Elliptic curve Diffie–Hellman. (n.d.). *Wikipedia*. Available: https://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman Accessed: Oct 17 2015

[8] Digital Signature Algorithm.(n.d.). *Wikipedia*. Available: https://en.wikipedia.org/wiki/Digital_Signature_Algorithm Accessed: Oct 17 2015

[9] D. Johnson, A. Menezes, S. Vanstone. (n.d.). The Elliptic Curve Digital Signature Algorithm (ECDSA). [Online]. Available: http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf Accessed: Oct 17 2015

[10] Elliptic Curve Digital Signature Algorithm. (n.d.).*Wikipedia*. Available: https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm Accessed: Oct 17 2015

[11] Network Associate. (1999). *PGP Software Developer's Kit User's Guide.* (v1.17). [Online]. Available: ftp://ftp.pgpi.org/pub/pgp/sdk/PGPsdkUsersGuide.pdf [Oct 17, 2015]

[12] Vidya G. (July 15th, 2013). Forensic Analysis of PGP-Encrypted Files. [Online]. Available: http://www.idrbt.ac.in/PDFs/PT%20Reports/2013/Vidya%20G_Forensic%20analysis%20of%20PGP-encrypted%20files_2013.pdf [Oct 17, 2015]

[13] *Elliptic curve cryptography*. Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Elliptic_curve_cryptography [Oct 17, 2015]

[14] N. Mavroyanopoulos and S. Josefsson. (October 17th, 2007) GNU TLS. (v2.0.2). [Online]. Available: http://ports.gnu-darwin.org/security/gnutls/work/gnutls-2.0.2/doc/gnutls.pdf

[15] NSS API Guidelines. *Mozilla*. Available: https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/NSS_API_GUIDELINES [Oct 17, 2015]

[16] Mozilla wiki. *PSM: CertPrompt*. [Online]. Available: https://wiki.mozilla.org/PSM:CertPrompt#Client_Authentication_Scenarios [Oct 17, 2015]

[17] PeerSec Networks. (2006). *MatrixSSL Developer's Guide*. (v1.8). [Online]. Available: http://cpansearch.perl.org/src/CDRAKE/Crypt-MatrixSSL-1.86.0/matrixssl-1-8-6-open/doc/MatrixSSLDeveloperGuide.pdf [Oct 17, 2015]

[18] U. Kumar et al. (Apr 16th, 2015). Comparative Analysis of Cryptography Library in IoT. [Online]. Available: http://arxiv.org/ftp/arxiv/papers/1504/1504.04306.pdf [Oct 17, 2015]

[19] Peter Gutmann. (April 2014).*Cryptlib Security Toolkit*. (v3.4.2). [Online]. Available: ftp://ftp.franken.de/pub/crypt/cryptlib/manual.pdf [Oct 17, 2015]

[20] WolfSSL. *Chapter 10: wolfCrypt (formerly CTaoCrypt) Usage Reference*. [Online]. Available:

https://www.wolfssl.com/wolfSSL/Docs-wolfssl-manual-10-wolfcrypt-usage-reference.html [Oct 17, 2015]