ECE 646 Fall 2015 project specification

Team: Ravi Kota.

Title: Overview, comparison of open crypto libraries for application development.

Introduction & Motivation:

There are many open source crypto libraries available. The purpose of this project is to study some of these open source crypto libraries, features, available literature on comparative analysis [1]-[6], internal organization of the libraries, APIs. Knowledge of internal organization of these libraries helps in cryptographic application design. Then identify/develop minimum requirement list, desirable features of common cryptography applications. Map these requirements to the internal features of the crypto libraries to compare them. Another feature to be investigated is list of vulnerabilities published in last 5 years and analyze which products are frequently impacted, and the type of vulnerability found, and reasons (such as implementation, weak algorithm etc.)

The uniqueness of this project is to complement the existing comparative analysis of some selected crypto libraries with the following additional attributes:

1. Define minimum set of requirements, and additional desirable features of common crypto applications, and hence to evaluate open source libraries using this criteria.
2. Study the internal library layers/structure of crypto libraries that might enable ease of use or flexibility for the target application.
3. Review the vulnerabilities published on these products, and analyze the root-cause or reason for such vulnerability, thus gives an idea on inherent strengths, weakness of crypto libraries.
4. Lastly a comment on the availability of documentation and support.

This information is very relevant in short listing the technologies (and thus defining the roadmap for organizations) to be evaluated and used in crypto applications in enterprises, organizations. The motivation for this study partly from my job, ideas generated while working on this topic.

1. Common minimum requirements of crypto application

Not much concise information is available about common minimum requirements for a crypto applications, which makes use of the crypto libraries to accomplish the task. This information is spread in some NIST documents [7], textbooks [8] and some in websites. Some of the requirements can be stated as below. This study is to identify & categorize the general requirements of crypto-applications.

I. Basic Cryptography Requirements

Requirements of symmetric key cryptography
Requirements of public key cryptography
Key Management
Random number generators
Security Requirements for Cryptographic Hash Functions
Message Authentication Requirements
Digital Signature Requirements

II. Software Integration Frameworks

How the software libraries utilize the OS level frameworks such as open-BSD framework [9], Crypto-API [10] cryptosystem building blocks and how they fit together.

III. Others (To be investigated)

The other requirements that might exist, shall be explored by reviewing use cases of popular applications built using open crypto libraries.

2. **Study of APIs crypto libraries**

   By understanding the crypto systems internal modules, APIs, layers and linking this information to the crypto-application requirements, very useful information can be derived about the application development using these libraries.

   The study of these libraries can be done using the available documentation, APIs [14]-[23].

3. **Study of the past vulnerabilities**

   Review the vulnerabilities on these products to identify the root cause of the vulnerabilities gives a valuable information the user of these libraries [24]. Examples are: CVE-2015-1793, CVE-2014-0160, CVE-2014-1568 etc.

4. **Support, availability of documentation, user guides**

   Availability of documentation, support plays a vital role in the success of application development using the open source libraries. The idea here is to explore the availability of documentation, user-guides, and examples of these products [14]-[23].

Open crypto libraries to be studied

C/C++ based Libraries

Nss (Network Security Services) 2:3.x
Openssl libraries 1.01
Crypto++ 5.6.2
Botan
AWS s2n library for TLS encryption

Java Based Libraries

Java SSL Library
GNU Crypto project
BouncyCastle

Others

These are scripting utilities that provide modules, APIs for cryptography functions. Brief overview of capabilities these two utilities will be explored.

PyCrypto - Python Cryptography Toolkit
Perl Crypto

Tentative Schedule:

	Task description	Date
1	Initial project specification	10/5/2015
2	Final project specification	10/17/2015

3.	Consolidated List of crypto application requirements	10/30/2015
4.	Detailed Review of APIs of Crypto Libraries	11/15/2015
5.	CVE Analysis - report	11/25/2015
6.	Draft Report	11/30/2015
7.	Review & Suggested Improvements and Report	12/09/2015

References:

[1] T. Bingmann at Permlink (2008, Jul 14) "Speedtest and comparison of open-source cryptography libraries and compiler flags". [Online]. Available: **https://panthema.net/2008/0714-cryptography-speedtest-comparison/**

[2].U. Kumar, T. Borgohain, S.Sanyal (2015, April 16) "Comparative analysis of cryptography library in IoT" [Online]. Available: **http://arxiv.org/ftp/arxiv/papers/1504/1504.04306.pdf**

[3] FedoraProject (2012, Mar 20) "Crypto consolidation eval" Fedora [Online]. Available: **https://fedoraproject.org/wiki/CryptoConsolidationEval**

[4] cURL (n.d.) "Compare ssl libraries" cURL (Online). Available: **http://curl.haxx.se/docs/ssl-compared.html**

[5] D. Dinu, A. Biryukov, J. Großsch¨adl, D. Khovratovich, Y. Le Corre, L. Perrin (2015, Jul 2015) "FELICS – fair evaluation of lightweight cryptographic systems" [Online]. Available**: http://csrc.nist.gov/groups/ST/lwc-workshop2015/presentations/session7-dinu.pdf** and **http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session7-dinu-paper.pdf**

[6] A. Stolarski(2012, Aug 23) "A review of selected cryptographic libraries" Hacking [Online]. Available: **http://resources.infosecinstitute.com/cryptographic-libraries/**

[7]. NIST (2014, March 4-5) "Cryptographic key management workshop" [online]. Available: **http://www.nist.gov/itl/csd/ct/ckm_workshop2014.cfm**

[8]. W. Stallings "Cryptography and Network Security: Principles and Practice", 6th ed. Prentice Hall, 2013, ISBN-13: 978-0133354690

[9]. Wikipedia (2015, March 5) "OpenBSD cryptographic framework". [Online]. Available: **https://en.wikipedia.org/wiki/OpenBSD_Cryptographic_Framework**

[10] Wikipedia (2015, August, 19) "Crypto api (linux)". [Online]. Available: **https://en.wikipedia.org/wiki/Crypto_API_%28Linux%29**

[11] M. D. Green (2013, Mar 13) "A few thoughts on cryptographic engineering." [Online]. Available: **http://blog.cryptographyengineering.com/2013/03/here-come-encryption-apps.html**

[12] D.J. Bernstein, T. Lange, and P. Schwabe, "The security impact of a new cryptographic library," in LNCS 7533, A. Hevia and G. Neven, Eds., Proc. LatinCrypt, Santiago, Chile, 2012, pp. 159–176. [Online]. Available: **http://cr.yp.to/highspeed/coolnacl-20120725.pdf**

[13] D. Ireland (2015 Sep 21) "Cryptography code." [Online]. Available: **http://www.di-mgt.com.au/crypto.html**

[14] Openssl cryptography ssl/tls toolkit (2015, July 9) [Online]. Available: **http://www.openssl.org/**

[15] Network security services (2014, Sep 7) [Online]. Available: **https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS**

[16] Botan crypto and tls for C++11 (2015, Aug 3) [Online]. Available: **http://botan.randombit.net/**

[17] Crypto++ library 5.6.2 (2015, Aug 15) [Online]. Available: **http://www.cryptopp.com/**

[18]. "AWS s2n open source TLS implementation" (1025, June 30). [Online]. Available: **https://blogs.aws.amazon.com/security/post/TxCKZM94ST1S6Y/Introducing-s2n-a-New-Open-Source-TLS-Implementation**

[19] H. Bedi "Java ssl library" [Online]. Availabe: **http://ssllib.sourceforge.net/**

[20] B.Ramprasad "GNU crypto project" (2006, Nov 25). [Online]. Available**:** http://www.gnu.org/software/gnu-crypto/

[21] "Bouncy castle crypto library" (n.d.) au Ceti Co-operative Ltd. [Online]. Available: **https: //www.bouncycastle.org/java.html**

[22] CPAN (n.d.) YellowBot. [online]. Available: **http://search.cpan.org/**

[23] D. Litzenberger "PyCrypto - Python Cryptography Toolkit" [Online]. Available: **https://www.dlitz.net/software/pycrypto/**

[24] "Common vulnerabilities and exposures" The Mitre Corporation. [Online]. Available: **https://cve.mitre.org/index.html**

[25] "NaCl: networking and cryptography library" RCRYPT. [Online]. Available: **http://nacl.cr.yp.to/features.html**

[26]. "SANS Institute" SANS [Online]. Available: **https://www.sans.org/**

[27]. "Guide to cryptography" (2015, Sep 12) OWASP. [Online]. Available: **https://www.owasp.org/index.php/Guide_to_Cryptography**

Report out line:

1. Summary of comparison of the open crypto libraries from the literature, and their supportability (availability of documentation, user-guides, examples etc)
2. Requirements of crypto applications
3. Internal library structure of open source libraries studied in this project (c/c++, java based)
4. Mapping the requirements to features available with crypto libraries (c/c++, java based)
5. Summary of features available in Python, Perl crypto modules

6. List of CVEs that impacted the open source libraries (c/c++, java based)
7. Conclusion