Cryptographic Libraries

Specification Report

Integrated Master in Informatics and Computing Engineering

Security in Computer Systems

Group 4:
João Fidalgo - 201303098
João Loureiro - 200806067
Ka Chon Ho - 201711244
Paulo Costa - 201206045

Faculdade de Engenharia da Universidade do Porto
Rua Roberto Frias, sn, 4200-465 Porto, Portugal

March 20, 2018

1 Introduction

Cryptology has quickly grown from a field only used by government and military agencies to being one that impacts the day to day lives of consumers across the globe. Cryptographic libraries are used by individuals in just about any country in the world when conducting secure online transactions, communicating via secure email or video, and in numerous B2B (business-to-business) transactions. As a result, there are a number of cryptographic libraries that have been developed for use in most of the major programming language libraries.[1]

2 Project Specification

2.1 Integration in Software

The Internet is a key to everything, especially e-whatever is a commonly used term in recently years, like "e-banking", "e-office". More and more data is being transferred through the Internet, which is a public network. Cryptography is used on these applications in order to prevent unexpected accesses, transactions, and operations. Our group would like to find out which is the most effective way of integrating the use of cryptographic libraries as well as the benefits and challenges of dealing with each if them.

2.2 Libraries Comparison

There will be made an extensive research about the existing cryptographic libraties, in order to find which one or which combination of them can provide the most value of use. In particular, there will be made a comparison between the cryptlib[2], openssl[3], NaCl[4] and gpl[5] libraries, among others that will be considered between the elements of the group. The main operations supported include key operations - key generation algorithms, key exchange agreements and public key cryptography standards, hash functions, MAC algorithms, cyphers and hardware-assisted support.

2.3 Goals and Quality

There will be made an analysis of the given cryptographic libraries in order to do a classification of quality of the features provided, relative to each other. It will also be our group's goal to provide a deeper explanation about the current state of art of the libraries, as well as the reason of their creation, objective and their procedures, from a conceptual point of view.

2.4 Heartbleed

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).[6]

As a bonus to our project we will also present a demonstration of the Heartbleed Bug.[7]

References

[1] tech-faq. *Cryptographic Libraries.* URL: `http://www.tech-faq.com/cryptographic-libraries.html`. (accessed: 20.03.2017).

[2] cryptlib. *Encryption Security Software Development Toolkit.* URL: `http://www.cryptlib.com`. (accessed: 20.03.2017).

[3] OpenSSL Software Foundation. *Welcome to OpenSSL!* URL: `https://www.openssl.org/`. (accessed: 20.03.2017).

[4] Daniel J Bernstein, Tanja Lange, and Peter Schwabe. “The security impact of a new cryptographic library.” In: *IACR Cryptology ePrint Archive* 2011 (2011), p. 646.

[5] GnuPG Project. *GnuPG - Libraries.* URL: `https://gnupg.org/software/libraries.html`. (accessed: 20.03.2017).

[6] Synopsys. *The Heartbleed Bug.* URL: `http://heartbleed.com/`. (accessed: 20.03.2017).

[7] sensepost. *Test for SSL heartbeat vulnerability (CVE-2014-0160).* URL: `https://github.com/sensepost/heartbleed-poc`. (accessed: 20.03.2017).