Hochschule Offenburg
offenburg.university

E+I Elektrotechnik und Informationstechnik

Generic Cryptographic Interface

Documentation Steve Wagner

January 14, 2016

Laboratory for Embedded Systems and Communication Electronics
Hochschule Offenburg
Prof. Axel Sikora
Andreas Walz

Statutory declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

Offenburg, _____ _____

Date Signature

Abstract

Contents

1. Introduction

1.1. Cryptography

1.2. SSL/TLS protocol

1.3. Why should EmbetterSSL used as an exemple of bad written programm

1.3.1. Size of functions

1.3.2. Usage of global variables as well as contexts

1.3.3. Bad usage of preprocessor includes

2. Motivation

3. Design

4. Cryptography in the TLS protocol

4.1. Handshake Protocol

4.2. Cryptographic parts in the Handshake Protocol

5. Creation of the Generic Cryptographic Interface

5.1. Principe of context

5.2. Key management

5.3. Principal functions needed in the interface

5.3.1. Hash

5.3.2. Signature

5.3.3. Generate key pairs

5.3.4. Diffie-Hellmann

5.3.5. Cipher

5.3.6. Pseudo-random number generator

6. Integration of the new interface in embetterTLS's project

6.1. old embetterTLS VS new embetterTLS

6.2. CryptoWrap Interface to Generic Crypto Interface

7. Implementation of LibTomCrypt Designer

7.1. embetterTLS as client

7.2. embetterTLS as server

Bibliography

[1] Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Berlin Heidelberg, Berlin; Heidelberg [u.a.], 2. corr. printing edition, 2010.

[2] Ph.D. Rolf, Oppliger. *SSL and TLS: Theory and Practice*. Artech House, eSECURITY Technologies; Beethovenstrasse 10; CH-3073; Gümligen; Switzerland, 2009.

Appendix

Appendix A.

Documentation of the Generic Cryptographic Interface

Link