



BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF INFORMATION TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF INTELLIGENT SYSTEMS

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

CONTINUOUS INTEGRATION SYSTEM FOR INTER-OPERABILITY OF TLS/SSL LIBRARIES

PRŮBĚŽNÉ TESTOVÁNÍ INTEROPERABILITY KNIHOVEN TLS/SSL

BACHELOR'S THESIS

BAKALÁŘSKÁ PRÁCE

AUTHOR

AUTOR PRÁCE

FRANTIŠEK ŠUMŠAL

SUPERVISOR

VEDOUCÍ PRÁCE

Ing. ALEŠ SMRČKA, Ph.D.

BRNO 2017

Abstract

The goal of this thesis is to implement a continuous integration system, which allows periodic and on-demand testing of provided Secure Socket Layer (SSL) / Transport Layer Security (TLS) libraries on supported systems, and to show the functionality and potential of such system by extending the existing interoperability test suite. The main benefit of this thesis is ensuring interoperability between the most popular SSL/TLS libraries during their development, and to discover potential issues in the shortest possible time. Presented results show found issues discovered by combining and using the implementation parts of this thesis on real world scenarios.

Abstrakt

Cílem této práce je implementace systému pro testování Secure Socket Layer (SSL) / Transport Layer Security (TLS) knihoven na podporovaných systémech a jeho využití na rozšířené sadě testů pro verifikaci jejich interoperability. Tento systém umožňuje jak průběžné testování, tak testování na vyžádání pro specifickou verzi knihovny. Hlavním přínosem této práce je zajištění interoperability nejznámějších SSL/TLS knihoven již ve fázi vývoje a detekce chyb v co nejkratším čase. Výsledky této práce ukazují nalezené problémy na skutečných případech využití těchto knihoven a jejich dopad na systém, kde jsou použity.

Keywords

testing, interoperability, TLS, SSL, continuous integration, CI

Klíčová slova

testování, interoperabilita, TLS, SSL, průběžná integrace, CI

Reference

ŠUMŠAL, František. *Continuous Integration System for Interoperability of TLS/SSL Libraries*. Brno, 2017. Bachelor's thesis. Brno University of Technology, Faculty of Information Technology. Supervisor Smrčka Aleš.

Continuous Integration System for Interoperability of TLS/SSL Libraries

Declaration

Hereby I declare that this bachelor's thesis was prepared as an original author's work under the supervision of Ing. Aleš Smrčka, Ph.D. The supplementary information was provided by Stanislav Židek and Hubert Kario. All the relevant information sources, which were used during preparation of this thesis, are properly cited and included in the list of references.

.....

František Šumšal

May 8, 2017

Acknowledgements

I would like to thank Ing. Aleš Smrčka, Ph.D. for his guidance in formal parts, structure and direction of this thesis, Stanislav Židek and Hubert Kario for their patience and incredible technical support during the entire course of this thesis, and Jakub Mach and Kamil Jeřábek for their moral and encouraging support when it was needed the most.

Contents

1	Introduction	3
1.1	Structure of the Document	3
2	Secure Sockets Layer / Transport Layer Security	4
2.1	Overview	4
2.2	TLS Protocols	5
2.2.1	TLS Record Protocol	5
2.2.2	TLS Handshake Protocol	6
2.2.3	TLS Change Cipher Spec Protocol	10
2.2.4	TLS Alert Protocol	10
2.2.5	TLS Application Data Protocol	10
2.3	Cipher Spec and Cipher Suite	10
2.4	TLS Extensions	11
2.4.1	Session Tickets	11
2.4.2	Signature Algorithms	11
2.5	Libraries	12
2.5.1	OpenSSL	12
2.5.2	NSS	13
2.5.3	GnuTLS	13
3	Implementation Details	14
3.1	Tested Environments	14
3.2	Test Format	14
3.2.1	Test relevancy	15
3.3	Tested Features	17
3.4	Continuous Integration System	17
3.4.1	GitHub & Webhooks	17
3.4.2	Jenkins	17
3.5	Final CI Implementation with Travis CI	19
3.5.1	Operating System	19
3.5.2	Test Environments	19
3.5.3	Test Execution	20
3.5.4	Performance and Limits	21
3.5.5	On-demand Library Compilation	21
3.6	Test Extension Details	22
3.6.1	GnuTLS	22
3.6.2	NSS	23
3.6.3	OpenSSL	24

3.7 Outstanding Issues(?)	24
4 Testing Results	25
4.1 NSS	25
4.2 GnuTLS	27
4.3 BeakerLib	27
5 Conclusion	28
Bibliography	29
Appendices	31
A TLS Alerts	32
B Test Plan	34
B.1 Test Plan Identifier	34
B.2 References	34
B.3 Introduction	34
B.4 Test Items	34
B.4.1 Components	34
B.4.2 Environments: Releases and Architectures	34
B.5 Software Risk Issues	35
B.6 Features to be Tested	35
B.7 Features not to be Tested	35
B.8 Approach	35
B.9 Item Pass/Fail Criteria	36
B.10 Test Cases	36
B.11 Suspension Criteria and Resumption Requirements	36
B.12 Test Deliverables	36
B.13 Remaining Test Tasks	37
B.14 Environmental Needs	37
B.14.1 Hardware	37
B.14.2 Software	37
B.15 Staffing and Training needs	37
B.16 Responsibilities	37
B.17 Schedule	38
B.18 Approvals	38
C Test Cases Description	39
C.1 GnuTLS	39
C.2 NSS	40
C.3 OpenSSL	40

Chapter 1

Introduction

SSL/TLS is the most widely used technology for securing today's Internet communications. Every application, which transmits data over the Internet, should implement some kind of encryption and many of these applications use SSL/TLS. But, as the correct way of implementing such encryption can be very tricky, and a simple mistake may have severe consequences, several general-purpose implementations – libraries – were created. These libraries allow the application to use SSL/TLS without having to create their own implementation.

Even though these libraries follow certain standards, which should ensure their interoperability (ability to communicate with any library which implements SSL/TLS according to the standards), they may contain little deviations or issues which can cause unexpected behavior or even some more serious problems (like denial of service). To avoid, or to at least detect, such issues, we can implement tests, which will test the interoperability between the SSL/TLS libraries. This is one of the main goals of this thesis.

Executing these tests manually for different environments would be ineffective, tedious and not error-prone. Thus, using an automation, which would test various combinations of different library versions on different versions of operating systems is necessary. Such automation – in this case we call it *continuous integration* – is the second main topic of this thesis.

By combining all these features together, we get a powerful system for continuous SSL/TLS library testing. Such system can be used for regression detection and ensuring, that interoperability between two given libraries works in a specific environment with a specific combination of settings.

1.1 Structure of the Document

All necessary components for such system are described in the following chapters, starting with a brief description of SSL/TLS protocols and their features in chapter 2.

Chapter ?? describes various continuous integration systems, which were considered for the final solution, and how the implemented solution looks like.

The testing itself, along with used technologies, is discussed in chapter ?. This chapter also includes a list and description of libraries, which were chosen to be tested and why.

During the testing phase several issues were found. Some of them are „harmless“, others can have a serious impact on the application, which uses given library. Summary of these results is detailed in chapter 4 following a thesis summary in chapter 5.

Chapter 2

Secure Sockets Layer / Transport Layer Security

Secure Sockets Layer (SSL) and its successor *Transport Layer Security* (TLS) are cryptographic protocols designed to provide communications security over a computer network. As the latest version of the SSL protocol (version 3.0 [2]) was deprecated in June 2015 [12] it will not be discussed further in this thesis.

Although there are currently three TLS versions – TLS 1.0 [16], TLS 1.1 [17] and TLS 1.2 [18] – this thesis focuses only on the latest two as TLS 1.0 is basically SSL 3.0 with a few differences. Also, there were few cryptographic problems found in TLS 1.0 and later resolved in TLS 1.1 (e.g. BEAST [7]).

2.1 Overview

The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications. The structure of the protocol comprises two layers: the TLS Record Protocol and the TLS Handshake Protocol.

The TLS Record Protocol lies at the lowest level, above some reliable transport protocol (e.g., TCP ¹). This protocol provides security which has following properties:

- The connection is private. Symmetric cryptography is used for data encryption (e.g., AES ², Camellia, 3DES ³, etc.). The keys for the symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol). The TLS Record Protocol can also be used without encryption.
- The connection is reliable. Message transport includes a message integrity check using a keyed MAC ⁴. Secure hash functions (e.g., SHA-1 ⁵, SHA-256, etc.) are used for MAC computations. The MAC is used to prevent undetected data loss or data modification during transmission.

¹Transmission Control Protocol

²Advanced Encryption Standard

³Triple DES (Data Encryption Standard)

⁴Message Authentication Code

⁵Secure Hash Algorithm

The TLS Record Protocol is used for encapsulation of various higher-level protocols. One such protocol is the TLS Handshake Protocol. This protocol allows client authentication and negotiation of necessary properties of the TLS connection, like encryption algorithm or cryptographic keys, before the data transmission. The TLS Handshake Protocol provides connection security which has following properties:

- The peer’s identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA ⁶, ECDSA ⁷, etc.). This authentication is not mandatory, but it is generally required for at least one of the peers.
- The negotiation of a shared secret is secure. Obtaining of the shared secret is infeasible for any eavesdropper or attacker, who can place himself in the middle of the authenticated connection.
- The negotiation is reliable. The negotiation communication cannot be modified without being detected by the parties to the communication. [18]

In addition to the properties above, a carefully configured TLS connection can provide another important privacy-related property: forward secrecy. This property ensures, that any future disclosure or leakage of encryption keys cannot be used to decrypt any TLS communications recorded or eavesdropped in the past.

TLS supports various combinations of algorithms for key exchange, data encryption and message integrity authentication, which is an important fact for this thesis and can cause severe issues when these combinations are configured or implemented improperly. Along with these combinations, TLS supports many extensions further extending its capabilities and possibilities, which will be described further in this thesis.

2.2 TLS Protocols

As mentioned above, the TLS protocol consists of four protocols – the TLS Record Protocol, the TLS Handshake Protocol, the TLS Changer Cipher Spec Protocol, the TLS Alert Protocol and the TLS Application Data Protocol. In this section we will overview and discuss these protocols in more detail.

2.2.1 TLS Record Protocol

In section 2.1 we briefly described the main function of the TLS Record Protocol, which is encapsulation of protocol data from higher layers. This includes fragmentation, optional compression, MAC application, encryption and transmission of the data. On the receiving side the data is decrypted, verified, decompressed, reassembled and then delivered to the higher layers.

Through the data processing, following TLS data structures are used – `TLSP Plaintext`, `TLSCompressed` and `TLSCiphertext`. At the end a TLS record is formed by appending an TLS record header to the `TLSCiphertext` structure.

⁶Rivest-Shamir-Adleman cryptosystem

⁷Elliptic Curve Digital Signature Algorithm

2.2.2 TLS Handshake Protocol

The TLS Handshake Protocol is the core protocol of TLS which operates on top of the TLS Record Protocol. Its goal is the authentication of communicating peers and negotiation of security parameters necessary for establishment or resumption of secure sessions.

The session establishment consists of following steps:

- Protocol version negotiation
- Cipher suite negotiation
- Server authentication and (optional) client authentication using digital certificates
- Exchange of session key information

The actual session establishment using the TLS Handshake Protocol proceeds as follows (see Figure 2.1):

1. The client sends a **ClientHello** message to the server, that includes the TLS version, a list of cipher suites supported by the client (in the client's order of preference) and the client's random value, which is used in subsequent computations.
2. The server responds with a **ServerHello** message, including the protocol version, the cipher suite chosen by the server, the session ID, and the server's random value.
3. If the server is to be authenticated, it sends its certificate in a **Certificate** message.
4. A **ServerKeyExchange** message may be sent if the client needs some additional information for the key exchange.
5. If the client authentication is required, the server sends a **CertificateRequest**.
6. Finally, the server sends a **ServerHelloDone** message, to indicate that the hello-message phase of the handshake is complete.
7. If the server has sent the **CertificateRequest** message, the client must send the **Certificate** message containing its certificate.
8. The client sends a **ClientKeyExchange** message. Its content depends on the chosen key exchange algorithm.
9. If the client has sent its certificate to the server, it must also send a digitally-signed **CertificateVerify** message, which explicitly verifies possession of the private key belonging to the client's certificate.
10. The client sends a **ChangeCipherSpec** message to the server, using the TLS Change Cipher Spec Protocol (see section 2.2.3) and copies its pending write state into the current write state, which makes the negotiated settings active.
11. The client sends a **Finished** message to the server under the new write state (with the new algorithms, keys, and secrets).
12. In response, the server sends its own **ChangeCipherSpec** message, copies its pending write state into the current write state and send the **Finished** message under the new cipher spec.



Figure 2.1: Full TLS handshake

Note: * marks messages which are sent only under specific conditions.

At this point, the TLS handshake is complete, and the peers may begin to exchange application layer data.

When the client and the server decide to resume a previous session or duplicate an existing one, the handshake can be simplified considerably (see Figure 2.2). The client sends a **ClientHello** message including the ID of the session to be resumed. The server then checks its session cache for a match. If a match is found, and the server is willing to re-establish the connection under the specified session state, it sends a **ServerHello** message with the same Session ID value. The client and the server can then directly move to the **ChangeCipherSpec** message followed by the **Finished** message. If a Session ID match is not found in the session cache, the server generates a new session ID and the peers perform a full TLS handshake.



Figure 2.2: Simplified TLS handshake

Let's have a closer look at the various messages that are exchanged during the TLS handshake:

HelloRequest

This message may be sent by the server at any time and tells the client to begin a new session negotiation. Client should respond to this message with a **ClientHello**. This message is not often used, but it can be useful in some cases, e.g. forcing a session renegotiation for a TLS sessions which are active for a longer period of time.

ClientHello

The **ClientHello** message is usually the first message in the TLS handshake, sent by the client, which initiates the session negotiation. The message itself contains the latest TLS version supported by the client, the client's random value, a session ID (which can be empty, if the client wishes to negotiate a new session), a list of supported cipher suites, a list of compression methods and optional extensions.

ServerHello

The **ServerHello** is the server's response to the client's **ClientHello** message. The structure of this message is quite similar to the **ClientHello** – instead of the lists of cipher suites and compression methods, the server specifies a single cipher suite and a single compression method. These values are chosen from the client's **ClientHello** message and will be used for the session. The complete message contains the TLS version chosen by the server, the server's random value, the length of the session ID and the session ID, the cipher suite, the compression method and the optional extensions.

Certificate

If the agreed-upon key exchange method uses certificates for authentication, the server sends a **Certificate** message containing a certificate chain. This certificate chain can be then used by the client, to verify the server's identity. The same message is used when a client authentication is required (as a response to a **CertificateRequest** message, see

below). All exchanged certificates are of X.509 v3 type [4], if not stated otherwise during the negotiation.

ServerKeyExchange

In some cases, the **Certificate** message does not contain enough data to allow the client to exchange a pre-master secret. In this situation, the server sends a **ServerKeyExchange** message with necessary cryptographic information, which allows such exchange and allows the client to complete the key exchange.

When RSA (or Diffie-Hellman with fixed parameters) is used, the client can retrieve the public key (or the server's Diffie-Hellman parameters) from the server certificate. In these cases the **Certificate** message is enough to complete a key exchange. But, for example, in case of ephemeral Diffie-Hellman, the client needs some additional information — Diffie-Hellman parameters — which must be delivered in a **ServerKeyExchange** message.

CertificateRequest

When the server wants to authenticate the client, it sends a **CertificateRequest** message to the client. This message tells the client which certificates are accepted by the server, and also asks the client to send its certificate to the server. Only a non-anonymous server can send a **CertificateRequest** — that means a server, which authenticates itself using the **Certificate** message.

ServerHelloDone

This message is sent by the server and indicates the end of the section of messages initiated by the **ServerHello** message. After sending this message, the server will wait for a client response.

ClientKeyExchange

The **ClientKeyExchange** message is sent by the client and it provides the server with the client-side keying material, which is used to generate the pre-master secret.

CertificateVerify

If the client provided a certificate that has a signing capability, it must prove that it holds the corresponding private key for that certificate. In this case, the client sends a digitally signed **CertificateVerify** message to the server. This allows the server to verify the client certificate using the client's public key and authenticate the client.

Finished

The **Finished** message is always sent immediately after a **ChangeCipherSpec** message 2.2.3 to verify that the key exchange and authentication processes were successful. As the message follows the **ChangeCipherSpec** message, it is the first message protected by the newly negotiated algorithms and keys.

2.2.3 TLS Change Cipher Spec Protocol

The TLS Change Cipher Spec Protocol is used to signal transitions in ciphering strategies. The protocol itself consists of a single compressed and encrypted message – **ChangeCipherSpec**. The encryption and compression methods correspond to the current (not the pending) cipher spec.

After receiving this message, the receiver instructs its record layer to immediately copy the read pending state into the read current state. Similarly, immediately after sending this message, the sender instructs its record layer to copy the write pending state into the write current state. All subsequent messages sent by the sender are then protected under the newly negotiated cipher spec.

2.2.4 TLS Alert Protocol

To exchange alert messages between peers, like warnings and errors, the TLS Alert Protocol is used. Each alert message has its severity (warning, fatal) and a description of the alert. All messages with an alert level of fatal result in the immediate termination of the connection.

The alert’s description field contains an identifier of the alert. These descriptions can be split into two categories – closure alerts and error alerts. The former one contains only one alert – **close_notify**. This message can be sent by either party and notifies the recipient that the sender will not send any more messages. Any data received after this message must be ignored. The knowledge of the fact, that the connection is ending, is crucial to avoid truncation attacks. The second category contains a number of error alerts used for various purposes during the TLS session. All TLS alert messages are summarized in Table A.1.

2.2.5 TLS Application Data Protocol

The TLS Application Data Protocol takes the arbitrary data from the application layer and feeds it into the TLS Record Protocol for fragmentation, compression and encryption. The resulting TLS records are then sent to the recipient.

2.3 Cipher Spec and Cipher Suite

In previous sections, terms *cipher spec* and *cipher suite* were mentioned. Let’s have a closer look at their meanings.

A *cipher spec* refers to a pair of algorithms that are used to cryptographically protect data. Such pair consists of a message authentication algorithm (*MAC*) and a data encryption algorithm. If we add a key exchange algorithm to a cipher spec, we get a *cipher suite*.

For example, *TLS_DHE_RSA_AES_256_CBC_SHA1* refers to a TLS cipher suite which uses ephemeral Diffie-Hellman with RSA for a key exchange, 256-bit AES in CBC ⁸ mode for encryption, and SHA-1 for message authentication.

⁸Cipher Block Chaining

2.4 TLS Extensions

As mentioned in section 2.2.2, the `ClientHello` and `ServerHello` messages contain an optional field for extensions. These extensions can be used to add functionality to TLS.

When a client wants to use an extension it sends its name in the `ClientHello` message. If the extension is supported by the server, it will be included in the responding `ServerHello` message. However, if the `ServerHello` message contains an extension, which was not sent by the client, the connection must be aborted with an `unsupported_extension` fatal alert (A.1). [14] [15]

Describing all currently implemented extensions [5] is way beyond scope of this thesis. Thus, in the following paragraphs we will discuss only those extensions, which are currently tested by the implementation part of this thesis. Nevertheless, support for other extensions is highly probable in the near future.

2.4.1 Session Tickets

If a client wanted to resume an existing session, it would have to send a session ID in its `ClientHello` message (field `session_id`) and the server would have to check its cache for a match (see section 2.2.2). This may cause problems on systems with a large amount of requests from different users or on systems with little memory. For such cases there is a `SessionTicket` TLS extension which uses client-side caching. [9]

In the initial handshake, where the client does not possess a ticket for an existing session, it includes an empty `SessionTicket` TLS extension in its `ClientHello` message. The server responds with an empty `SessionTicket` extension to indicate that it will send a new session ticket using the `NewSessionTicket` message. This ticket contains the current session state (such as cipher suite and master secret) and is cryptographically protected by a key, which is known only to the server.

When the client wishes to resume the session, it includes the cached ticket in the `SessionTicket` extension of its `ClientHello` message. The server then decrypts and verifies the contents of the ticket and resumes the session according to the decrypted parameters. If the server cannot, or does not want to use the state from the ticket, it can initiate a full handshake with the client.

2.4.2 Signature Algorithms

TLS 1.2 defines ([18], section 7.4.1.4.1) an extension `supported_signature_algorithms`, which allows the client to tell the server which hash and signature algorithm combinations it supports. Even though internally the supported algorithms are split into two lists (none, MD5, SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 for hash algorithms and anonymous, RSA, DSA and ECDSA for signature algorithms), the algorithms sent in the extension are always listed in pairs, as not all combinations may be accepted by an implementation.

The peers exchange this information through the `ClientHello` and `ServerHello` messages including the `supported_signature_algorithms` extension. The client sends a list of supported algorithms and the server responds with its choice, that is going to be used for any subsequent signature generation and verification.

2.5 Libraries

To prevent each project implementing the SSL/TLS on its own and introducing (in many situations) dangerous issues, several libraries were created and can be used by any project, which needs a SSL/TLS support. The most popular ones are OpenSSL ⁹, NSS ¹⁰ and GnuTLS ¹¹. Although, there are other SSL/TLS libraries (e.g. LibreSSL ¹² or BoringSSL ¹³), this thesis aims only on these three. However, a future expansion to support other libraries is not impossible.

Even though these libraries are separate projects, an user of such library must be able to communicate with every client, which supports the particular protocol and cipher suite, no matter which implementation they use. Testing of this functionality — *interoperability* — is the main goal of this thesis.

For the testing itself we need at least two applications - a client and a server. One option would be writing these applications from scratch, using the public API ¹⁴ of each library, which is not error prone and would require a maintenance of such applications. Thankfully, each of the tested libraries provides a set of utilities, among which we can find a simple client and server applications with dozens of settings and options. These utilities are then used in various scenarios to ensure, that given valid combination of settings works for both client and server using different libraries.

2.5.1 OpenSSL

OpenSSL is an open source library maintained by The OpenSSL Project, which provides a toolkit for SSL and TLS protocols, along with other general-purpose cryptographic functions.

This library provides a single powerful utility called *openssl*. This utility has dozens of sub-commands with various SSL/TLS related functionality, where the most important ones are:

ciphers information about supported cipher suites

dsa, rsa, ec DSA/RSA/EC key management

s_client a simple SSL/TLS client

s_server a simple SSL/TLS server

x509 X.509 certificate data management

Thanks to its functionality-rich interface, OpenSSL is used for certificate generation and management for all libraries in the testing process.

⁹<https://www.openssl.org/>

¹⁰<https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS>

¹¹<https://www.gnutls.org/>

¹²<https://www.libressl.org/>

¹³<https://boringssl.googlesource.com/boringssl/>

¹⁴Application Programming Interface

2.5.2 NSS

Network Security Services (NSS) is a set of open source libraries providing support for SSL and TLS protocols, S/MIME ¹⁵ and other optional features, like server-side TLS/SSL acceleration or client-side hardware smart cards support.

Compared to OpenSSL, which has a single utility for everything, NSS does the exact opposite – each feature or tool has its own utility. For our testing purposes, we will need the following ones:

certutil certificate and key management for NSS databases

listsuities information about supported cipher suites

selfserv a simple SSL/TLS server

strscInt a simple SSL/TLS client for performance testing

tstclnt a simple SSL/TLS client

This library differs from the other two in the way how it handles server and client certificates. These certificates cannot be passed directly as arguments to the utility, but must be imported to a NSS database which is then passed as an argument to the utility.

2.5.3 GnuTLS

GnuTLS is a secure communications library which implements SSL, TLS and DTLS ¹⁶ protocols.

Like the the libraries above, GnuTLS includes several utilities for library testing - GnuTLS client *gnutls-cli* and GnuTLS server *gnutls-serv*. Both utilities support a parameter **-l**, which lists all necessary information about supported cipher suites.

¹⁵Secure/Multipurpose Internet Mail Extensions

¹⁶Datagram Transport Layer Security

Chapter 3

Implementation Details

Following sections describe in detail the most important part of this thesis – implementation of the continuous integration system, test extension, and how these two parts work together to ensure interoperability of SSL/TLS libraries.

As the majority of the tests for this thesis were not developed from scratch, section 3.6 contains a comprehensive review of things which were added throughout the implementation of this thesis.

3.1 Tested Environments

For the purposes of this thesis, an environment consists of an operating system (e.g. CentOS¹, Fedora²) and its version (e.g. 7, 25). Each of these environments must be tested separately, as it contains a different set of library versions and policies, which affect the SSL/TLS communication.

This thesis covers SSL/TLS libraries on CentOS and Fedora, as the tests used and extended by this thesis were originally created for RHEL³.

3.2 Test Format

Each test consists of two main files – *runtest.sh* and *Makefile* – and other optional auxiliary files. *Makefile* contains metadata of the particular test, such as its name, author, version, dependencies, information about relevancy, package it tests, etc. It also contains several make targets, so for example `make run` makes the *runtest.sh* executable and runs it. The CI makes use of this file and extracts some necessary information from it – namely dependencies and relevancy – to ensure correct execution of the test itself.

The second file – *runtest.sh* – is the core of the test. It is a Bash script using the BeakerLib⁴ testing framework containing a sequence of commands and asserts which are executed and evaluated. Each command execution or an assert creates a record in a log, which is processed, stored and printed at the end of each test run.

Let's have an example *runtest.sh* script, which simply generates an elliptic curve key and checks if it contains „BEGIN EC PRIVATE KEY“ (Figure 3.1). When executed, BeakerLib

¹<https://www.centos.org/>

²<https://getfedora.org/>

³Red Hat Enterprise Linux - <https://www.redhat.com/en/technologies/linux-platforms/enterprise-linux>

⁴<https://github.com/beakerlib/beakerlib>

```

. /usr/share/beakerlib/beakerlib.sh || exit 1

PACKAGE="openssl"

rlJournalStart
    rlPhaseStartSetup
        rlAssertRpm $PACKAGE
        rlRun "TestDir=$(pwd) "
        rlRun "TmpDir=$(mktemp -d) " 0 "Creating tmp directory "
        rlRun "pushd $TmpDir "
    rlPhaseEnd

    rlPhaseStartTest
        rlRun "openssl ecparam -genkey -name prime256v1 -out ec.key "
        rlAssertGrep "BEGIN_EC_PRIVATE_KEY" "ec.key "
    rlPhaseEnd

    rlPhaseStartCleanup
        rlRun "popd "
        rlRun "rm -r $TmpDir" 0 "Removing tmp directory "
    rlPhaseEnd
rlJournalPrintText
rlJournalEnd

```

Figure 3.1: Example runtest.sh file

generates two logs – the first one is generated throughout the test execution and contains outputs of all executed commands, whether the second one is generated at the end of the test and contains a summary of the first log. An execution log can be seen in Figure 3.2.

3.2.1 Test relevancy

To control in which environments should be each test case executed, we have to implement an algorithm, which would check if a given test case is relevant for a given environment before the execution itself. The information about relevant environments is stated in the Makefile of each test case and has a following format:

```
" Releases:          -RHEL4 -RHELClient5 -RHELServer5 "
```

The test will be excluded from all environments, which have a - symbol before their name. Environments not included in the list are implicitly added when the final check is done. The same syntax can be used for architectures as well, but as the current CI is limited to an x86_64 architecture, it is not relevant for this thesis.

To apply this relevancy during the testing itself a simple script was created, which parses the Makefile and compares the parsed environments with the current one. If a match with a non-excluded environment is found, the test is executed, otherwise it is simply skipped.

As the CentOS and RHEL environments are basically the same, the relevancy script is able to interchange between these two environments to avoid unnecessary duplicites in the Makefile. Thus, a RHEL7 environment from the Makefile matches both CentOS 7 and RHEL 7 environments.

```

::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
:: [ LOG ] :: Setup
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::

openssl-1.1.0c-5.fc26.x86_64
:: [ PASS ] :: Checking for the presence of openssl rpm
:: [ 22:32:45 ] :: Package versions:
:: [ 22:32:45 ] :: openssl-1.1.0c-5.fc26.x86_64
:: [ BEGIN ] :: Running 'TestDir=$(pwd)'
:: [ PASS ] :: Command 'TestDir=$(pwd)' (Expected 0, got 0)
:: [ BEGIN ] :: Creating tmp directory :: actually running
:: [ PASS ] :: 'TmpDir=$(mktemp -d)'
:: [ BEGIN ] :: Creating tmp directory (Expected 0, got 0)
:: [ BEGIN ] :: Running 'pushd /tmp/tmp.qHTxIVtyY2'
/tmp/tmp.qHTxIVtyY2 /tmp
:: [ PASS ] :: Command 'pushd /tmp/tmp.qHTxIVtyY2'
:: [ PASS ] :: (Expected 0, got 0)

::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
:: [ LOG ] :: Test
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::

:: [ BEGIN ] :: Generate an EC key :: actually running
:: [ PASS ] :: 'openssl ecparam -genkey -name prime256v1
:: [ PASS ] :: -out ec.key'
:: [ PASS ] :: Generate an EC key (Expected 0, got 0)
:: [ PASS ] :: File 'ec.key' should contain 'BEGIN EC PRIVATE KEY'

::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
:: [ LOG ] :: Cleanup
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::

:: [ BEGIN ] :: Running 'popd'
/tmp
:: [ PASS ] :: Command 'popd' (Expected 0, got 0)
:: [ BEGIN ] :: Removing tmp directory :: actually running
:: [ PASS ] :: 'rm -r /tmp/tmp.qHTxIVtyY2'
:: [ PASS ] :: Removing tmp directory (Expected 0, got 0)

```

Figure 3.2: Execution log of the runtest.sh from Figure 3.1

3.3 Tested Features

Each library goes through several layers of testing:

- **Basic interoperability** – Simple communication without any special settings
- **Session resumption** – Verify if session resumption works (Section 2.2.2); this test is done twice – with Session IDs and with SessionTicket extension (Section 2.4.1)
- **Session renegotiation** – Verify if session renegotiation works (Section 2.2.2)
- **signature__algorithms*** – Verify if signature__algorithms extension works (Section 2.4.2)

* This test is (so far) not implemented for all supported libraries, as some of them lack necessary support on CentOS.

All mentioned tests are performed multiple times – with and without client certificates, with and without TLSv1.2 enabled, and for each supported ciphersuite.

Apart from these tests, each tested combination has a *Common Criteria* test ⁵ which test the necessary subset of functionality which is required to work according to the library specifications and standards.

3.4 Continuous Integration System

As manual testing is often tedious and not error prone, an automated system has to be implemented to test a developed component both periodically and on-demand, when developer requests it. Such system should be capable of running all relevant tests on given component without (almost) any manual intervention and reporting results back to the person, who requested it. [3]

During the progress of this thesis, we tried several solutions before implementing and accepting the final one.

3.4.1 GitHub & Webhooks

First of the proposed solutions was a simple Python script, which would make use of GitHub's webhooks [8]. This script would listen for requests from GitHub and would perform required tasks.

This solution, even though it was very flexible, would require re-implementation of many things already implemented in already existing solutions, which would consume unnecessary amount of time, that could be utilized for other, more important things.

3.4.2 Jenkins

During the search for more robust and complete solution, we came across Jenkins. Jenkins is an open-source automation server, which can be used for automation of various tasks [10]. After several proof-of-concept solutions we knew that Jenkins is something we can build on.

⁵<https://www.commoncriteriaportal.org/>

Nevertheless, Jenkins itself lacks integration with GitHub. Thankfully, that could be solved by using several open-source plugins. First of them is *GitHub Plugin* ⁶, which provides basic integration with GitHub and functionality for other GitHub plugins. This functionality is used and improved by *GitHub pull request builder plugin* ⁷, which adds support for polling from GitHub webhooks, trigger hooks for specific comments in pull requests, customizable build status messages and others.

Combining all these things above together, we were able to create a working automation system – *CI* – which reacted to changes in the test repository and reported build results back to it. The major disadvantage was in running all build tasks on the same machine as the Jenkins itself. So the another necessary task was implementing some kind of isolation for the build tasks.

In our current infrastructure we use Beaker (Section 3.4.2) for machine provision, where each tasks (or a set of tasks) has its own machine. This sounded like exactly what we needed, but that would require obtaining machines for a machine pool and their maintenance, which was far too excessive for a such small project.

Taking inspiration from another of our internal projects, we thought about using OpenStack (Section 3.4.2) for provision of virtual machines. OpenStack could run on the same machine as Jenkins, so we would not need another hardware. Also, the provision can be done from pre-installed images, so it would be much faster than in case of Beaker. Unfortunately, after spending several hours by reading documentation and playing around with OpenStack itself, we have concluded, that it would be too demanding to maintain.

Finally, we managed to isolate build tasks using Docker containers (Section 3.4.2). But, after this step, where we managed to get rid of dependency on other machines, and basically on dependency on the underlying operating system itself, we were trying to move everything somewhere to the cloud, so we would be free of the need of maintaining our own infrastructure. And thankfully, after another trial and error, we managed to accomplish that goal using Travis.

Beaker

Beaker is an open-source software for managing and automating labs of test computers. [13] It allows administrators and users to maintain an automated inventory of all machines present in the machine pool with system details, running tasks on machines with specific environments and reporting (and storing) results back.

OpenStack

OpenStack is an open-source cloud operating system for managing pools of compute, storage, and networking resources. [11] For easier administration and usage, almost everything can be managed through a web dashboard, which provides all necessary information. OpenStack itself consists of several components, which can be added or removed according to the particular needs.

Docker

Docker is an open-source project which automates deployment of applications inside containers. [6] Container is a small, executable image, which contains all necessary software

⁶<https://wiki.jenkins-ci.org/display/JENKINS/GitHub+Plugin>

⁷<https://wiki.jenkins-ci.org/display/JENKINS/GitHub+pull+request+builder+plugin>

to run a desired application without any other external dependencies, in an isolated environment. This approach allows an user to run an application under a different operating system – e.g. running an application in a CentOS 7 container even though the host operating system is Ubuntu. This feature is crucial in the CI implemented in this thesis.

3.5 Final CI Implementation with Travis CI

As mentioned above, the chosen solution is Travis CI. Travis CI is a powerful, hosted, distributed continuous integration service, used exclusively to build and test projects hosted at GitHub. [19] It has two variants – commercial, for private projects and free, for open-source projects. As all tests and scripts from this thesis are open-source, and we were already using GitHub, we could use the free variant and throw away the need for our own infrastructure.

After hooking a repository to Travis, it reacts to all commits, branches and pull requests, for which a new build is created. Status of each build is reported back to GitHub in two ways – for commits it is an icon in their summary (yellow dot for a running build, green tick for a passed build and red cross for a failed build), and for pull requests it is located in the information box of each pull request. Both ways contain a hyperlink to the particular build with general overview and status with logs for each job (environment).

Nevertheless, even though Travis CI met our expectations, it was not exactly „out-of-the-box“ solution, as several obstacles had to be overcome.

3.5.1 Operating System

First major issue was the OS used by Travis CI, which is Ubuntu, as our tests should run on CentOS and Fedora. Thankfully, using and extending the already implemented solution from the previous experience with Jenkins, we were able to work around this issue using Docker containers. Both CentOS ⁸ and Fedora ⁹ have official images for Docker, so we did not have to bother with making and maintaining our own Docker images.

Travis CI itself supports Docker, so we can simply tell Travis to enable Docker for our build, pull a correct docker image and then simply run whatever we want inside the container.

3.5.2 Test Environments

Even though Travis does know the concept of environments, and has a built-in mechanism for specifying a matrix of environment variables, where each set specifying an environment has its own job, it still needs some handler, which would correctly set up the environment according to these settings.

For this purpose, a short Bash script was written ¹⁰. This script takes four arguments – OS type (centos, fedora), OS version (7, 25, ...), tested component (openssl, gnutils, nss) and glob pattern for further test case specification (see Section 3.5.4).

Before executing the tests itself, several preparation steps need to be made to install and configure all necessary dependencies. First of them is library certgen ¹¹, written by Hubert Kario, for generating certificates, which are later used in the testing process.

⁸https://hub.docker.com/_/centos/

⁹https://hub.docker.com/_/fedora/

¹⁰`scripts/test-setup.sh`

¹¹<https://github.com/redhat-qe-security/certgen>

The second dependency, or to call it properly – the second workaround, is creating a fake library for FIPS ¹² configuration, as FIPS is not supported by Travis (yet). When this library is loaded properly, it configures system into a FIPS mode. Current solution just returns zero (success) without any changes to the underlying system, which allows us running tests even in Travis without FIPS support.

The last thing before the Docker execution itself is checking each test for `rlGetTestState` command. This command must be present as the last thing in each test, as all BeakerLib tests return zero even if they contain failed phases. Ensuring, that each test has this command at its end, gives us relevant results from each test, as `rlGetTestState` returns a number of failed phases as the script's exit code (or 255 if the number of failed phases is bigger than 255). [1]

After the preparations, a docker container is executed with given environment settings and the `scripts/test-runner.sh` script as an entry point. This script will be described in detail in the following section.

3.5.3 Test Execution

As the test suite contains several tests, where each one of them lies in its own script file, it does not have any entry point, which could be passed to Docker to run all tests. For this case, a script ¹³ had to be created, which would coordinate test execution according to the current environment.

This script has the same arguments as the `test-setup.sh` – OS type, OS version, component and test glob – which are used to determine a package manager (yum on CentOS or dnf on Fedora), correct OS version (Docker images support a „latest“ tag, which needs to be translated to an exact version), and whether to configure EPEL ¹⁴ repository, as BeakerLib is not in base repositories on CentOS.

As these test were originally developed for RHEL (and still are), another workaround had to be implemented to avoid complex branching in the tests. BeakerLib has a function `rlIsRHEL`, which allows certain phases to be run only on some version of RHEL – e.g. condition `if rlIsRHEL 6; then ...` would execute a code inside of the if statement only on RHEL 6. But this function does not work on CentOS. For CentOS, there is a conveniently named function `rlIsCentOS`, which does the same thing. To avoid having to use both functions for each if statement, the `test-runner.sh` creates a wrapper function `rlIsRHEL` which overloads the original function. The overloaded function then simply calls `rlIsCentOS`, so the tests can use the RHEL function only.

Next step is a full system upgrade, as the Docker images are usually not up to date, followed by installation of basic dependencies necessary for the test execution.

The core of the test runner scripts consist of a loop, which goes through all tests for given component. If the test passes through all relevancy checks, it is executed, otherwise it is skipped.

The first relevancy check is via the previously mentioned glob pattern, which uses extended globbing feature of Bash. This glob pattern is then simply matched with the test case name – if it matches, the test continues to the next relevancy check, otherwise it is skipped.

¹²Federal Information Processing Standard - <http://csrc.nist.gov/groups/STM/cmvp/standards.html>

¹³`scripts/test-runner.sh`

¹⁴<https://fedoraproject.org/wiki/EPEL>

The second check is a comparison of OS version and OS type with metadata from the test's Makefile (see Section 3.2.1). For this purpose we have a script `scripts/relevancy.awk` written, as the name suggests, in GNU AWK ¹⁵. This script, apart from the comparison itself, performs necessary substitutions between RHEL and CentOS to give correct results.

If a test passes through all relevancy checks, its Makefile is parsed once again for dependencies (section *Requires*). These dependencies are installed and the test is executed.

The test runner keeps statistics of executed, skipped and failed tests, which are logged along the test results and can be viewed in the Travis web UI.

3.5.4 Performance and Limits

During the CI development, we found out about several limiting factors in Travis, which had to be solved. Some of them are related only to the free version of Travis CI (for open-source projects), and some of them affecting all Travis versions.

First one is a time limit per job, which is 50 minutes. At the beginning of this thesis this was not an issue, as there was a quite big reserve in this matter. Nevertheless, as more and more test combinations were added, this limit was hit several times.

Originally, each OS type and version has its own job, so there was one job for CentOS 6, one for CentOS 7 and one for the latest Fedora. The first step of solving the aforementioned issue was creating a separate job for each OS type, version and component combination. This resulted in nine jobs (GnuTLS, NSS and OpenSSL times supported operating systems) which were enough, at least for a while.

As another batch of changes was added, the limit was hit again on Fedora along with another, previously unknown limit – the size of the result log – which is 4 MiB. After several proposed solutions we decided to add another variable to the environment definition – `test glob` – which allows splitting each component test suite internally into smaller pieces, depending on their name. This solution proved to be quite effective and should last for a while (until we reach another milestone, where one test runs for more than 50 minutes).

3.5.5 On-demand Library Compilation

To be able to call this system a „continuous integration system“, there had to be a way how to test a development version of a SSL/TLS library. This appeared to be a complicated issue, as Travis itself does not support monitoring of external repositories, thus it is not able to tell whether a new change was committed to such repository. ¹⁶

As stated in previous sections, any dependency on an external infrastructure is an unwanted solution (e.g. an external watchdog). Thus, after several proposals, a semi-automated solution was implemented, which consists of a small configuration file, containing a path to a repository with target SSL/TLS library, a branch, which contains desired library version, and a library identifier.

If such configuration file exists, the `test-runner.sh` script 3.5.3 tries to read it and if it is a valid configuration, it passes all parsed information to the `scripts/lib-compile.sh` script. This script contains recipes for all supported libraries, as each library has a custom way of compilation and installation. If the compilation fails, the job is immediately aborted and a build log is printed to the resulting log to be analysed. Otherwise, the test runner continues as usual with execution of all relevant tests for given environment.

¹⁵<https://www.gnu.org/software/gawk/>

¹⁶<https://github.com/travis-ci/travis-ci/issues/631>

This solution has a few disadvantages – the library is compiled in each job, which is unnecessary, and it requires a separate branch to be created manually by a developer, with the custom configuration file. The first issue is particularly hard to solve, as the jobs does not have any shared space, and usually run in paralel. The second issue it not easy to solve without incorporating some kind of external system or watchdog. As this implementation is currently being discussed and tested by developers, it is possible it will be improved or replaced completely in the future.

3.6 Test Extension Details

As this thesis started with already existing tests (and its purpose was to extend them), following paragraphs should make clear what was already implemented and what is the result of this thesis.

3.6.1 GnuTLS

gnutls/renegotiation-with-NSS

New features:

- Use certgen library for generating certificates
- Test 20 ciphersuites instead of only the default one
- Test renegotiation scenarios with client certificates

Overall stats: 457 additions, 32 deletions

gnutls/renegotiation-with-OpenSSL

New features:

- Use certgen library for generating certificates
- Test 20 ciphersuites instead of only the default one
- Test renegotiation scenarios with client certificates

Overall stats: 399 additions, 24 deletions

gnutls/resumption-with-NSS

New features:

- Create certificate PKI
- Test 20 ciphersuites instead of only the default one
- Test resumption scenarios with client certificates and with SessionTicket extension

Overall stats: 469 additions, 35 deletions

gnutls/resumption-with-OpenSSL

New features:

- Use certgen library for generating certificates
- Test 20 ciphersuites instead of only the default one
- Test resumption scenarios with client certificates and with SessionTicket extension

Overall stats: 425 additions, 29 deletions

gnutls/signature__algorithms-with-OpenSSL

[[finish when the test is done]]

gnutls/TLSv1-2-with-NSS

New features:

- Explicitly enable RC4 and DHE-DSS
- Temporarily ignore crypto-policies on Fedora

Overall stats: 13 additions, 6 deletions

gnutls/TLSv1-2-with-OpenSSL

New features:

- Explicitly enable RC4 and DHE-DSS

Overall stats: 7 additions, 6 deletions

3.6.2 NSS

nss/CC-nss-with-gnutls

New features:

- Explicitly enable RC4 and DHE-DSS

Overall stats: 10 additions, 3 deletions

nss/Interoperability-with-OpenSSL

[[find out what happened with the WIP version]]

nss/renego-and-resumption-NSS-with-OpenSSL

New features:

- OpenSSL-NSS - basic interoperability
- OpenSSL-NSS - basic interoperability with client certificates
- NSS-OpenSSL - fixed basic interoperability
- NSS-OpenSSL - fixed basic interoperability with client certificates
- NSS-OpenSSL - session renegotiation
- NSS-OpenSSL - session renegotiation with client certificates
- NSS-OpenSSL - session resumption
- NSS-OpenSSL - session resumption with client certificates
- Add missing expect scripts

Overall stats: 343 additions, 61 deletions

3.6.3 OpenSSL

openssl/CC-openssl-with-gnutls

New features:

- Explicitly enable RC4 and DHE-DSS

Overall stats: 9 additions, 2 deletions

3.7 Outstanding Issues(?)

[[FIPS]]

[[REF: <https://www.nist.gov/information-technology-laboratory/fips-general-information>]]

[[expect scripts - random hangups, unreliability, ...]]

Chapter 4

Testing Results

Throughout the test extension process, several bugs and issues were found in the tested libraries, as well as in the auxiliary utilities. These issues have various levels of security impact and will be described in detail in this chapter.

Described issues have following format:

Issue ID(s)

[severity, affected systems]

Issue summary

Issue description

<version>: <link to component's issue tracker>

Issue ID abbreviations:

CVE Common Vulnerabilities and Exposures ¹

BZ Red Hat bug-tracking system ²

MBZ Mozilla bug-tracking system ³

4.1 NSS

CVE-2016-9574, BZ#1397482, BZ#1397410

[Urgent, RHEL/CentOS 6, RHEL/CentOS 7]

Segfault in selfserv during session handshake when using SessionTicket extension and ECDHE-ECDSA ciphersuites

selfserv utility crashes during handshake when using SessionTicket extension for session resumption. This issue although does not occur when using client certificates.

CVE: <https://access.redhat.com/security/cve/CVE-2016-9574>

RHEL/CentOS 6: https://bugzilla.redhat.com/show_bug.cgi?id=1397482

RHEL/CentOS 7: https://bugzilla.redhat.com/show_bug.cgi?id=1397410

¹<https://cve.mitre.org/>

²<https://bugzilla.redhat.com/>

³<https://bugzilla.mozilla.org/>

BZ#1426182, MBZ#1320695

[Urgent, RHEL/CentOS 7, upstream]

Support ticket based session resumption using only ECDSA certificate

Using SessionTicket extension along with any ECDHE-ECDSA ciphersuite renders `selfserv` server unusable.

RHEL/CentOS 7: https://bugzilla.redhat.com/show_bug.cgi?id=1426182

Upstream: https://bugzilla.mozilla.org/show_bug.cgi?id=1320695

BZ#1436114, MBZ#1350950

[Unspecified, RHEL/CentOS 7, upstream]

Sending of CERTIFICATE REQUEST messages does not correspond to manual

When `-r` or `-rr` parameter is used with `selfserv` utility, to request (and require) client certificate on initial handshake, the CERTIFICATE REQUEST message is sent on both handshakes, whereas when `-rrr` or `-rrrr` parameter is used, the CERTIFICATE REQUEST message is not sent at all. This does not correspond to the manual of the `selfserv` utility, which states following:

`-r` flag is interpreted as follows:

- 1 `-r` means request, not require, cert on initial handshake.
- 2 `-r`'s mean request and require, cert on initial handshake.
- 3 `-r`'s mean request, not require, cert on second handshake.
- 4 `-r`'s mean request and require, cert on second handshake.

RHEL/CentOS 7: https://bugzilla.redhat.com/show_bug.cgi?id=1436114

Upstream: https://bugzilla.mozilla.org/show_bug.cgi?id=1350950

BZ#1397486, BZ#1397472, MBZ#1320708

[Low, RHEL/CentOS 6, RHEL/CentOS 7, upstream]

strscInt gets stuck during session resumption when using client certificates

`strscInt` utility gets stuck during session resumption (for both SessionTicket and SessionID) when using client certificates and when the server has enabled client certificate verification.

RHEL/CentOS 6: https://bugzilla.redhat.com/show_bug.cgi?id=1397486

RHEL/CentOS 7: https://bugzilla.redhat.com/show_bug.cgi?id=1397472

Upstream: https://bugzilla.mozilla.org/show_bug.cgi?id=1320708

BZ#1397478, BZ#1397365

[Low, RHEL/CentOS 6, RHEL/CentOS 7]

NSS session resumption using session ID does not work for DHE-DSS ciphersuites

When NSS acts as a server, session resumption using SessionID does not work for ciphersuites using DHE-DSS algorithm. Even though this behavior is expected for the ticket based resumption, the Session ID resumption should work.

RHEL/CentOS 6: https://bugzilla.redhat.com/show_bug.cgi?id=1397478

RHEL/CentOS 7: https://bugzilla.redhat.com/show_bug.cgi?id=1397365

BZ#1426267

[Unspecified, Fedora 25]

Broken Crypto Policy handling of RC4 ciphersuites

On F25 RC4 ciphers in NSS should be disabled by Crypto Policy, but in the current version it works only partially - when NSS acts as a client, the handshake fails, but when it acts as a server, the handshake is completed successfully.

Fedora 25: https://bugzilla.redhat.com/show_bug.cgi?id=1426267

4.2 GnuTLS

BZ#1401564

[Unspecified, RHEL/CentOS 7]

Duplicate PK signature algorithms in gnutls-cli output

Output of `gnutls-cli -l` command contains duplicate public key signature algorithms – namely SIGN-RSA-SHA1 and SIGN-RSA-MD5.

RHEL/CentOS 7: https://bugzilla.redhat.com/show_bug.cgi?id=1401564

BZ#1434091, BZ#1434420

[Unspecified, RHEL/CentOS 7]

Session renegotiation fails with client certificates

GnuTLS sends a client certificate in renegotiation, even if it was not requested by the server, causing the handshake to fail.

RHEL/CentOS 7: https://bugzilla.redhat.com/show_bug.cgi?id=1434091

Fedora 25: https://bugzilla.redhat.com/show_bug.cgi?id=1434420

4.3 BeakerLib

BZ#1416014

[High, upstream]

rlWaitForSocket -close now waits for incorrect socket

A patch in the latest testing version of beakerlib causes that `rlWaitForSocket -close` can cause a deadlock/unwanted delay, because of grepping an incorrect socket.

Upstream: https://bugzilla.redhat.com/show_bug.cgi?id=1416014

Chapter 5

Conclusion

[[summarize findings, current CI state, future work (if any), ...]]

Bibliography

- [1] *beakerlib(1) Linux User's Manual*. January 2017.
- [2] A. Freier, P. Karlton, P. Kocher: The Secure Sockets Layer (SSL) Protocol Version 3.0. RFC 6101. RFC Editor. August 2011.
Retrieved from: <https://www.rfc-editor.org/rfc/rfc6101.txt>
- [3] Amazon Web Services, Inc.: What is Continuous Integration? 2017.
Retrieved from: <https://aws.amazon.com/devops/continuous-integration/>
- [4] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280. RFC Editor. May 2008.
Retrieved from: <https://www.rfc-editor.org/rfc/rfc5280.txt>
- [5] D. Eastlake: Transport Layer Security (TLS) Extensions: Extension Definitions. RFC 6066. RFC Editor. January 2011.
Retrieved from: <https://www.rfc-editor.org/rfc/rfc6066.txt>
- [6] Docker Inc.: Docker Documentation. 2017.
Retrieved from: <https://docs.docker.com/>
- [7] Duong, T.; Rizzo, J.: Here Come The XOR Ninjas. 2011.
- [8] GitHub Inc.: Webhooks. 2017.
Retrieved from: <https://developer.github.com/webhooks/>
- [9] J. Salowey, H. Zhou, P. Eronen, H. Tschofenig: Transport Layer Security (TLS) Session Resumption without Server-Side State. RFC 5077. RFC Editor. January 2008.
Retrieved from: <https://www.rfc-editor.org/rfc/rfc5077.txt>
- [10] Jenkins Infra: Jenkins Documentation. 2017.
Retrieved from: <https://jenkins.io/doc/>
- [11] OpenStack: OpenStack Docs. 2017.
Retrieved from: <https://docs.openstack.org/>
- [12] R. Barnes, M. Thomson, A. Pironti, A. Langley: Deprecating Secure Sockets Layer Version 3.0. RFC 7568. RFC Editor. June 2015.
Retrieved from: <https://www.rfc-editor.org/rfc/rfc7568.txt>
- [13] Red Hat, Inc.: Administration Guide. 2017.
Retrieved from: <https://beaker-project.org/docs/admin-guide/>

- [14] S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen, T. Wright: Transport Layer Security (TLS) Extensions. RFC 3546. RFC Editor. June 2003.
Retrieved from: <https://www.rfc-editor.org/rfc/rfc3546.txt>
- [15] S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen, T. Wright: Transport Layer Security (TLS) Extensions. RFC 4366. RFC Editor. April 2006.
Retrieved from: <https://www.rfc-editor.org/rfc/rfc4366.txt>
- [16] T. Dierks, C. Allen: The TLS Protocol Version 1.0. RFC 2246. RFC Editor. January 1999.
Retrieved from: <https://www.rfc-editor.org/rfc/rfc2246.txt>
- [17] T. Dierks, E. Rescorla: The Transport Layer Security (TLS) Protocol Version 1.1. RFC 4643. RFC Editor. April 2006.
Retrieved from: <https://www.rfc-editor.org/rfc/rfc4346.txt>
- [18] T. Dierks, E. Rescorla: The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246. RFC Editor. August 2008.
Retrieved from: <https://www.rfc-editor.org/rfc/rfc5246.txt>
- [19] Travis CI, GmbH: Travis CI User Documentation. 2017.
Retrieved from: <https://docs.travis-ci.com/>

Appendices

Appendix A

TLS Alerts

Table A.1: TLS Alerts

Alert	ID	Description
close_notify	0	The sender notifies the recipient that it will not send any more messages on this connection.
unexpected_message	10	An inappropriate message was received. This alert is always fatal.
bad_record_mac	20	The sender received a record with an incorrect MAC. This alert is always fatal.
decryption_failed_RESERVED	21	Used in some earlier versions of TLS, must not be sent by compliant implementations.
record_overflow	22	A <code>TLSCiphertext</code> record was received that had a length more than $2^{14} + 2048$ bytes or a record decrypted to a <code>TLSCompressed</code> record with more than $2^{14} + 1024$ bytes. This alert is always fatal.
decompression_failure	30	The decompression function received improper input. This alert is always fatal.
handshake_failure	40	The sender was unable to negotiate an acceptable set of security parameters given the options available. This alert is always fatal.
no_certificate_RESERVED	41	This alert was used in SSLv3 but it no longer used in any TLS version.
bad_certificate	42	The sender notifies the recipient that the provided certificate is corrupt.
unsupported_certificate	43	The sender notifies the recipient that the provided certificate is of an unsupported type.
certificate_revoked	44	The sender notifies the recipient that the provided certificate was revoked by the issuing authority.
certificate_expired	45	The sender notifies the recipient that the provided certificate has expired or is no longer valid.
certificate_unknown	46	The sender notifies the recipient that some unspecified issue occurred during the certificate processing, rendering it unacceptable.

Table A.1: TLS Alerts

Alert	ID	Description
<code>illegal_parameter</code>	47	A field in the handshake was out of range or inconsistent with other fields. This alert is always fatal.
<code>unknown_ca</code>	48	The received certificate could not be validated, because the CA certificate could not be located or could not be matched with a known, trusted CA. This alert is always fatal.
<code>access_denied</code>	49	A valid certificate was received, but when access control was applied, the sender decided not to proceed with negotiation. This alert is always fatal.
<code>decode_error</code>	50	The received message could not be decoded because some field was out of the specified range or length of the message was incorrect. This alert is always fatal.
<code>decrypt_error</code>	51	A handshake cryptographic operation failed. This alert is always fatal.
<code>export_restriction_RESERVED</code>	60	Used in some earlier versions of TLS, must not be sent by compliant implementations.
<code>protocol_version</code>	70	The protocol version the client has attempted to negotiate is recognized but not supported. This alert is always fatal.
<code>insufficient_security</code>	71	The server requires more secure ciphers than those supported by the client. This alert is always fatal.
<code>internal_error</code>	80	An internal error occurred, unrelated to the peer or correctness of the protocol. This alert is always fatal.
<code>user_canceled</code>	90	This handshake is being canceled for some reason unrelated to a protocol failure. This alert should be followed by a <code>close_notify</code> .
<code>no_renegotiation</code>	100	The peer should respond with this alert when renegotiation is not appropriate regarding the current connection state. This alert is always a warning.
<code>unsupported_extension</code>	110	Sent by the client when the received <code>ServerHello</code> message contains an extension not sent by the client in its <code>ClientHello</code> message. This alert is always fatal.

Appendix B

Test Plan

B.1 Test Plan Identifier

TLS/SSL Interoperability Test Plan v0.1

B.2 References

- IEEE 829-2008 Standard for Software Test Documentation ¹
- Common Criteria access.redhat.com ²

B.3 Introduction

The main goal of this test plan is to ensure interoperability of supported SSL/TLS libraries on CentOS/RHEL and Fedora systems. The testing itself involves verification of ability to communicate between two libraries using various combination of cipher suites, connection settings and extensions.

B.4 Test Items

B.4.1 Components

- OpenSSL
- NSS
- GnuTLS

B.4.2 Environments: Releases and Architectures

Due to limitations of the current CI all tests are run on x86_64 architecture only. Nevertheless, they should work on all architectures supported by the underlying operating system.

- CentOS 6 and 7 (latest releases)
- Fedora (latest release)

¹<http://standards.ieee.org/findstds/standard/829-2008.html>

²<https://access.redhat.com/blogs/766093/posts/1976523>

B.5 Software Risk Issues

- Package rebases can cause unexpected behavior and/or regressions – thorough test results analysis is necessary

B.6 Features to be Tested

All features are tested using TLSv1.1 and TLSv1.2 protocols with all supported cipher suites by the involved parties.

- Basic interoperability
- Interoperability with client certificates
- Session renegotiation
- Session renegotiation with client certificates
- Session resumption using Session ID
- Session resumption using Session ID with client certificates
- Session resumption using TLS SessionTicket Extension
- Session resumption using TLS SessionTicket Extension with client certificates
- SignatureAlgorithms TLS Extension

B.7 Features not to be Tested

- Sanity of the available options
- Regressions
- Security of the implementation

B.8 Approach

All testing is done by Bash scripts using Beakerlib ³ testing framework. This framework manages log collection and results reporting and automatizes the entire testing process.

Each library has a set of utilities, which are used for the interoperability testing itself:

- **OpenSSL** – `openssl` utility (package *openssl*)
- **NSS** – utilities `selfserv`, `tstclnt`, `strsclnt`, etc. (package *nss-tools*)
- **GnuTLS** – utilities `gnutls-cli` and `gnutls-serv` (package *gnutls-utils*)

All libraries are tested in pairs in a client-server fashion, where each phase tests a specific combination of parameters (specific cipher suite, protocol, extension, etc.).

Each failure is investigated and if it is a library issue, it is reported to the upstream and/or to a respective downstream bug tracker.

³<https://github.com/beakerlib/beakerlib>

B.9 Item Pass/Fail Criteria

A handshake is completed successfully in all cases with all requested settings set, i.e.:

- Expected cipher suite is used
- Expected protocol is used
- A specific extension requested in Client/Server Hello is used
- Session is correctly resumed when session resumption is requested
- Session renegotiation is successful

B.10 Test Cases

Table B.1: Test case matrix

Test case	CentOS 6	CentOS 7	Fedora
gnutls/renegotiation-with-NSS		x	x
gnutls/renegotiation-with-OpenSSL		x	x
gnutls/resumption-with-NSS		x	x
gnutls/resumption-with-OpenSSL		x	x
gnutls/signature_algorithms-with-OpenSSL		x	x
gnutls/softhsm-integration		x	x
gnutls/TLSv1-2-with-NSS	x	x	x
gnutls/TLSv1-2-with-OpenSSL	x	x	x
nss/CC-nss-with-gnutls		x	x
nss/CC-nss-with-openssl		x	x
nss/Interoperability-with-OpenSSL	x	x	x
nss/rengo-and-resumption-NSS-with-OpenSSL	x	x	x
openssl/CC-openssl-with-gnutls		x	x

Brief description of all test cases can be found in [Appendix C](#).

B.11 Suspension Criteria and Resumption Requirements

Testing will be suspended if any of the following criteria are met:

- Underlying operating system is not installable
- Existing issues may prevent execution of the test suite

Testing will be resumed when all mentioned issues are resolved.

B.12 Test Deliverables

The test results generated by Beakerlib will be stored in the CI and all failures will be analysed. The analysis itself can yield following results:

- Failure caused by the tested component – a new bug will be reported
- Failure caused by the test – the test case will be fixed
- Failure caused by an error in the infrastructure/environment – the test case will be run again

B.13 Remaining Test Tasks

Extend test coverage to other TLS extensions:

- `extended_master_secret` extension
- `encrypt_then_mac` extension
- etc.

Implementation of tests for these extension is currently blocked on the limited support of these extensions by the utilities of SSL/TLS libraries.

Testing of some recent algorithms for TLS should be considered as well (e.g. *ChaCha20-Poly1305*⁴). This will have to wait until the SSL/TLS libraries provide support for these algorithms.

B.14 Environmental Needs

B.14.1 Hardware

Testing will be performed on `x86_64` architecture as it is the only architecture supported by the current CI. Particular hardware configuration is not important for the testing itself.

B.14.2 Software

No special configuration of the operating system is needed. All packages necessary for the testing will be installed by the CI system.

B.15 Staffing and Training needs

N/A

B.16 Responsibilities

- František Šumšal
- Stanislav Židek
- Hubert Kario

⁴<https://www.rfc-editor.org/rfc/rfc7905.txt>

B.17 Schedule

[[Update schedule => +periodic runs, +devel branches]] Currently all tests are being executed when a new PR or commit is pushed to the test repository. In the nearest future, all tests should be executed periodically, and when a new version of a supported system is released.

Long term plans include delivering all test cases to both downstream and upstream, so possible failures can be detected before the library itself is released.

B.18 Approvals

- Stanislav Židek

Appendix C

Test Cases Description

Note: the term „various cipher suites“ used in following sections describes cipher suites using different key exchange algorithms (RSA, DHE, ECDHE), authentication algorithms (RSA, DSA, ECDSA), block cipher algorithms (3DES, AES) and message authentication algorithms (SHA). Mentioned algorithms may also differ in modes (AES-GCM, AES-CBC, ...) and sizes (AES-128, AES-256, SHA-1, SHA-256, ...).

C.1 GnuTLS

renegotiation-with-NSS

Test session renegotiation between GnuTLS and NSS libraries using various cipher suites, TLSv1.1 and TLSv1.2 protocols, and client certificates.

renegotiation-with-OpenSSL

Test session renegotiation between GnuTLS and OpenSSL libraries using various cipher suites, TLSv1.1 and TLSv1.2 protocols, and client certificates.

resumption-with-NSS

Test session resumption between GnuTLS and NSS libraries using various cipher suites, TLSv1.1 and TLSv1.2 protocols, and client certificates. The resumption itself is tested using both Session IDs and SessionTicket extension.

resumption-with-OpenSSL

Test session resumption between GnuTLS and OpenSSL libraries using various cipher suites, TLSv1.1 and TLSv1.2 protocols, and client certificates. The resumption itself is tested using both Session IDs and SessionTicket extension.

signature_algorithms-with-OpenSSL

Test signature_algorithms extension in communication between GnuTLS and OpenSSL libraries with and without client certificates. This extension is present only in TLSv1.2 and higher. As this extension has to be explicitly enabled, it is currently tested only in this combination of libraries, due to lack of support in testing utilities provided by the libraries.

TLSv1-2-with-NSS

Verify interoperability of GnuTLS with NSS using TLSv1.2 protocol with various cipher suites.

TLShv1-2-with-OpenSSL

Verify interoperability of GnuTLS with OpenSSL using TLSv1.2 protocol with various cipher suites.

C.2 NSS**CC-nss-with-gnutls**

Test interoperability of cipher suites relevant for Common Criteria certification between NSS and GnuTLS libraries with and without client certificates.

CC-nss-with-openssl

Test interoperability of cipher suites relevant for Common Criteria certification between NSS and OpenSSL libraries with and without client certificates.

Interoperability-with-OpenSSL

Test interoperability between NSS and OpenSSL libraries using certificates generated by NSS (all other tests use certificates generated by OpenSSL). This test is currently under heavy refactoring as it was originally developed for RHEL 6.

renego-and-resumption-NSS-with-OpenSSL

Test session renegotiation and session resumption between NSS and OpenSSL libraries. Both methods are tested using various cipher suites, TLSv1.1 and TLSv1.2 protocols, and client certificates. Moreover, session resumption is tested using both Session IDs and SessionTicket extension.

C.3 OpenSSL**CC-openssl-with-gnutls**

Test interoperability of cipher suites relevant for Common Criteria certification between OpenSSL and GnuTLS libraries with and without client certificates.