Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 19, 2007

Y. Pettersen
Opera Software ASA

October 16, 2006

Clientside interoperability experiences for the SSL and TLS protocols draft-ietf-tls-interoperability-00

Status of this Memo

Copyright Notice

Abstract

This document presents a number of problems encountered when implementing TLS 1.0, TLS 1.1 and TLS Extensions for clients, and their consequences. The problems include servers that refuse to connect with clients supporting newer versions of the protocol, or that do not handle such negotiation properly. Another problem encountered is the incorrect use of values in the protocol messages.

Table of Contents

1. Introduction

One of the basic foundations of the various SSL protocol versions SSL v2 [SSLv2], SSL v3.0 [SSLv3], TLS 1.0 [RFC2246] and TLS 1.1 [RFC4346] is that they are supposed to be able to work seamlessly with other implementations of both older versions of the protocol, and newer versions that were not even under consideration at the time the implementation was written. The older versions are not supposed to be able to understand the new protocol versions, but using their version of the protocol, they are supposed to be able to negotiate a connection with the newer version, provided that the newer implementation is willing and able to do so. That ability may depend on both the implementer's willingness to support the older versions due to engineering constraints and known security problems with the older version. But, assuming that both implementations support the same version of the protocol, they should be able to communicate.

Over the years it has become an unfortunate reality that while most SSL and TLS implementations do work together in the above mentioned ideal fashion, there are far too many implementations that do not (in particular) properly implement the forward compatibility portions of the specifications. This has caused a number of serious problems which again may have led client vendors to delay implementation or deployment of new TLS-related functionality or versions. Other vendors may have deployed the new features, but have only been able to do so by adding automatic workarounds that in many respects actually disable security features of the protocol.

Even if one discounts the fact that SSL v2 and SSL v3 were incompatible at the binary level, with every upgrade since; the migration from SSL v3 to TLS 1.0, the addition of TLS Extensions and the current migration from TLS 1.0 to TLS 1.1, clients have encountered servers that were not willing to accept connections from clients that supported these features.

To make matters worse, from the client vendor's viewpoint, many of

the sites causing these problems are sites that are vital to their customers, such as banking and shopping sites.

This document will present a number of the implementation mistakes that have been observed throughout the author's period as the lead developer of an SSL/TLS client. In most cases one has knowledge only about what happened, not the precise reason why. The cases listed here are not intended as an exhaustive list of problems that have occurred in implementations of the SSL/TLS protocol, but to give an overview of what the situation is.

Finally, there will be a short evaluation of what may have caused the

current situation, and a few suggestions about what may be done to avoid these problems in the future, both for TLS and other protocols.

2. The SSL v3 to TLS 1.0 transition

The SSL v3 specification [SSLv3] includes the following version forward compatibility and security features:

- A field in the Client Hello that tells the server the highest version the client supports. If the server supports a more recent version than the client does, then it is supposed to select the client's version, otherwise it is to use its own highest supported version.

- A field in the RSA Client Key Exchange message that contains the highest version the client supports. The server must check this version number against the version number received in the Client Hello. If it is different, somebody may have attempted to reduce the security of the connection by downgrading the negotiated version.

These two features were intended to make it possible for implementations using newer SSL/TLS versions to connect to older implementations, and vice versa.

Unfortunately, a number of server implementations got at least one of those points wrong. Some SSL v3 servers refuse to even answer when a client using TLS 1.0 or higher tries to establish a connection,

others answer, but the negotiation fails after the RSA Client Key Exchange step because they use the negotiated version number, not the version number in the Client Hello, to check the version number in the RSA Key Exchange block.

Appendix A.1 and Appendix A.2 contain a couple of examples of the first type of problem, refusal to talk to TLS 1.0 clients. In these cases, the server usually closes down the connection immediately without an error code, although in some cases they do send an error first.

In the second type of problem the server correctly chooses SSL v3 as the version, but the last part of the handshake fails because the server assumes that the decrypted RSA Key Exchange message should contain the SSL v3 protocol version, not the TLS 1.0 version number (which is the correct one). In such cases the server also closes the connection. An example of a similar case, involving a TLS 1.1 client and a TLS 1.0 server is found in Appendix A.6.

To be able to connect to these servers clients have had to restart the negotiation on a new connection, with TLS 1.0 disabled, an action which for the RSA cipher suites mean that the version roll back protection is non-existent.

In addition to the above examples, a SSL v3 server that used whatever version the client identified in the Client Hello Version field as the version selected in the Server Hello has also been observed. That is, if the client identified {3,0} as its highest version the server selected (correctly) {3,0}, but if the client identified {3,1} or (the unspecified) {4,0} (Appendix A.8) the server selected {3,1} and {4,0}, respectively, even though it could not know what those protocol versions were. This incorrect version selection will invariably result in a handshake failure during the Client Key Exchange phase or a MAC/decryption failure during the decryption of the Finished Message

When the client used the SSL v2 Client Hello the version was correctly negotiated, which lead this problem being hidden until TLS 1.0 clients recently stopped using the SSL v2 Client Hello in the initial connection and started using the TLS 1.0 (or later) Client Hello instead, as part of the transition to support TLS

ExtensionsSection 4. As the server would previously only see a SSL v3.0 Client Hello after the client had determined the server supported SSL v3.0 as its highest version, such as during session resume or renegotiation, the server would only see a SSL v3.0 version number from the client. It is likely that the vendor, as part of mistaken optimization, just copied the version field into the session's state without checking that the version was the correct one.

3. The TLS 1.0 to TLS 1.1 transition

TLS 1.0 [RFC2246] also contained the same forward compatibility and version roll-back attack protections as SSL v3, and given the more formal specification of TLS 1.0, one might have hoped vendors would have taken better care to implement those specified provisions, so that a future transition from TLS 1.0 to TLS 1.1 [RFC4346] would work better.

Again, however, a number of TLS server vendors did not implement these aspects properly, and in many cases it is not possible to tell what is causing the problem, the web server, or a gateway server between the client and the web server.

Appendix A.3 shows a couple of cases where the server shuts down the connection immediately when it gets a Client Hello containing a TLS

1.1 version number. Similarly to the SSL v3 to TLS 1.0 transition servers using the wrong version number during the Client Key Exchange step have also been observed, as seen in Appendix A.6.

While many of the servers just close the connection, there are also some TLS 1.0 servers that fall back to SSL v3 when being contacted by a TLS 1.1 client.

4. The introduction of TLS Extensions

SSL v3 [SSLv3], TLS 1.0 [RFC2246] , and TLS 1.1 [RFC4346] all specify the possibility of an extension of the Client Hello to contain more information. This extension was defined with the TLS Extensions specification [RFC3546].

TLS Extensions defines a field containing a sequence of data items that inform the server about the client's capabilities and/or requirements. Two such fields are the Server Name Extension and the Certificate Status Extension, which can be used, respectively, to tell the server which server the client wants to connect to, allowing virtual server hosting for secure servers, and request that the server provides an OCSP response for the server's certificate.

As with the negotiation of version number, not all server implementations have taken these requirements into consideration, and in many cases TLS 1.0 servers will refuse to accept connections from clients that send TLS Extensions in the Client Hello, usually indicated by closing the connection without sending any error message. It was already known before work on TLS Extensions started that some SSL v3 servers would not tolerate the extended Client Hello used by TLS Extensions, even though the SSLv3 specification mentions the possibility of such an extension of the protocol.

Various scenarios have been observed:

- Some servers accept TLS Extensions with TLS 1.0, but refuse to accept them from TLS 1.1 clients
- Some servers accept TLS Extensions only from a TLS 1.1 client
- Some servers refuse to accept TLS Extensions under any circumstances.

Failures are usually signalled by closing the connection, optionally with an error alert, but servers that did not respond, leaving the connection open, have also been observed.

In at least one case, the reason for the first scenario seems to be that the server incorrectly used the Record Protocol version number as the negotiation input for version number, not the Client Hello version number field, and for version 3.2 reclassified it as 3.0 (not 3.1, as it should have), and then refused to accept the extended record, even if SSL v3 permits extended records.

Similar handling, but with more "graceful" recovery may be the reason

for the second scenario.

The third case, by far the most common, may be caused by incorrect understanding of the specification, but it may also be the result of misguided efforts at protecting the server from an attack by using data format rules in the firewall that are too restrictive. An indication of the latter is that the server in Appendix A.3 originally only refused to accept connection requests from a TLS 1.1 client, but four weeks after the site was first tested, it was no longer accepting TLS Extension requests (Appendix A.4). However, it has not been possible to confirm or refute this theoretical possibility.

5. Incorrect use of Record Protocol version numbers

Three incorrect uses of the SSL/TLS protocols Record Protocol version numbers has been observed, one server side, and two client side. These have not had much impact until recently (2005) because most SSL and TLS clients have been using the SSL v2 Client Hello to provide backward compatibility with servers that only supports SSL v2. As these servers are being upgraded, the need for this backward compatibility is diminishing, and most clients are now disabling this protocol in their default configuration, and they are therefore starting to use the SSL v3 and later Client Hellos in the initial handshake.

The first incorrect use concerns which Record Protocol version number to use in the initial connection. A single sentence in Section E of [RFC2246] covers this area, and specifies that "TLS clients who wish to negotiate with SSL 3.0 servers should send client hello messages using the SSL 3.0 record format and client hello structure, sending {3, 1} for the version field to note that they support TLS 1.0".

What this implies (in the author's current, revised understanding) is that the client should use the server's highest known version number in the first handshake (which would mean SSL v3.0 when there is no information available about the server).

At the very least, the author of this document missed the

significance of this sentence. It had not had any significance when

clients were using SSL v2 handshakes initially, since during future handshakes the client would know which version the server supported. It did however turn out to have some impact on some, but not all, of the problems with TLS 1.1 described above.

Changing the negotiation sequence to use SSL v3's 3.0 version number in the initial SSL/TLS record did, however, turn out to reveal another incorrect use of the Record Protocol version number: Some servers use it as the Client's Requested SSL/TLS protocol version-field instead of the Client Hello message field.

This means that a client using an SSL v3.0 record to request a TLS 1.0 connection from a TLS 1.0 capable server in some cases actually got an SSL v3 connection instead. Curiously, it does not seem like the RSA Client Key Exchange test for version roll-back triggered, probably because the implementations did use the correct field to retrieve the version number used in that check, but did not check it against the negotiated version number.

In other cases, such as in Appendix A.1 a SSL v3 server will not accept the TLS 1.0 version number in the protocol record, and will shut down the connection without any warning.

In some cases this use of the Record Protocol field has had some curious effects. In one case, if the client used the TLS 1.1 version number (3.2) while connecting to the server, the server would negotiate SSL v3.0, even though it did support TLS 1.0. This caused (as described above) the server not to accept TLS Extensions when the TLS 1.1 Record Protocol was used.

The third case concerned a client with which the author is not associated. This client would negotiate a TLS 1.0 session using a SSL v3 Record Protocol message with a Client Hello requesting TLS 1.0. Once the TLS session was negotiated, the client sent a new Client Hello, presumably to renegotiate the connection without revealing any of the exchanged information to eavesdroppers. It did this in the TLS 1.0 session, using a 3.0 Record Protocol version.

Apparently this worked in many cases, but in the case of two financial websites they returned errors when the client sent their second Client Hello, one of them a normal TLS error code, the other (the same one as in Appendix A.3 and Appendix A.4) actually responded with an SSL v2 error code Appendix A.5, which the client naturally wasn't able to understand.

6. Introducing Compression

[RFC3749] introduced new compression capabilities to TLS. The compression capability, which is intended to reduce bandwidth requirments, was documented already in [SSLv3], but until RFC3749 no compression methods, beside the Null method (no compression), had been defined. SSL v3 and all versions of TLS clearly specified that the list of compression methods was the list of methods (including the Null method) supported by the client, in order of preference, and that the server must select one of them among those it supports.

Clients and servers should therefore always be able to negotiate a compression method, even if it is the Null method.

Testing performed by Pasi Eronen have, however, indicated that at least one server implementation (Appendix A.7) does not accept connections from clients that offer to do any kind of compression in addition to the Null method.

7. Consequences

As a consequence of the problems detailed above, many mass-market client vendors have had to deploy SSL/TLS implementations that disable protocol features if the server does not understand it. In particular, this was necessary both for the move to TLS 1.0, and to TLS 1.1, but it has also become necessary for TLS Extensions.

The reason for this automatic disabling of features is that most of these clients cannot refuse to connect to an SSL/TLS server whose "only" problem is that it refuses to connect to a client that supports a feature it does not support.

The consequence, however, is that (at the very least) some security features in the protocol, such as the version roll-back protection (in the RSA-suites), are effectively disabled, because it is impossible for a client to distinguish between a non-compliant server and a malicious attack. A related issue is that only the RSA suites defined in TLS have any version roll-back protection that does not depend on the security of the message digest functions.

As long as SSL v3, TLS 1.0 and TLS 1.1 are as similar as they are, and relying on the same methods, this probably does not reduce the security of the protocol. However, as future versions of TLS are unlikely to rely solely on the same mechanisms as the current versions of TLS due to attacks on those mechanisms becoming more

feasible, the possibility of a version roll-back attack becomes more realistic.

8. What should be done?

Even though SSL and TLS clearly specified forward compatibility requirements in the specifications, a significant number of implementers did not implement them properly. Similarly, a number of implementers got some of the backwards compatibility guidelines wrong.

Many of these problems may have been caused, however indirectly, by the amount of detail in the specifications, which is unavoidable in any specification of some size. It may be possible to counter that category of problems by organizing the documents differently, such as by adding sections that summarizes important parts of the protocol.

Other problems may have been introduced because of external concerns, such as security.

What can be done to improve the situation, for TLS, as well as other protocols?

This document will not be able to provide the answer to that, but brings up the following questions:

- Should important aspects of a protocol be collected in an implementer's checklist?
- Should forward and backward compatibility requirements be better documented, e.g. by examples?
- Should specifications include reference implementations? If so, who should develop them?
- Should such reference implementations also include tests that break border conditions?
- Should the IETF host reference implementations?
- Can and should future TLS implementations contain Key Exchange-independent version roll-back protection? (Currently only the RSA

suites in [SSLv3], [RFC2246] and [RFC4346] have such protection)

- Is it feasible for future TLS specifications to require that implementations must never automatically fall back to an earlier version of the protocol, in case negotiation fails?

9. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

10. Security Considerations

This document discusses various problems with the implementations of the SSL and TLS protocol versions, and the interaction between implementations of newer and older versions of this protocol. The solution to some of the problems discussed can have security implications, such as when a client automatically disables its support for a version of the protocol or a feature in the protocol when it encounters a problem with a server.

11. Acknowledgements

Many of the sites exhibiting the problems discussed above and used in some of the examples were originally discovered by external testers of the Opera Browser, such as the Elektrans and those who participated in the September 2004 My Opera TLS 1.1 Scavenger Hunt, and employees of Opera Software ASA.

The example in Appendix A.7 was contributed by Pasi Eronen.

12. Normative References

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[RFC3546] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 3546, June 2003.

[RFC3749] Hollenbeck, S., "Transport Layer Security Protocol Compression Methods", RFC 3749, May 2004.

[RFC3943] Friend, R., "Transport Layer Security (TLS) Protocol Compression Using Lempel-Ziv-Stac (LZS)", RFC 3943, November 2004.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[SSLv2] Feb18, "The SSL Protocol", Feb 1995, <http://wp.netscape.com/eng/security/SSL_2.html>.

[SSLv3] "The SSL Protocol Version 3.0", Nov 1996, <http://wp.netscape.com/eng/ssl3/draft302.txt>.

Appendix A. Examples

A.1. SSL v3 server refuses TLS 1.0 client(case 1)

This server accepted connections from TLS 1.0 clients on one of two conditions

1. The Client used an SSL v2 Client Hello record

2. The client used an SSL v3 record protocol record to send the Client Hello with the TLS 1.0 version number.

A.1.1. Failed connection

This example shows a handshake started with TLS 1.0 Client Hello in a TLS 1.0 record, the result being that the server terminates the connection immediately.

```
 C: sending 82 bytes (Client Hello)
0000 : 16 03 01 00 4d 01 00 00 49 03 01 44 2c 2d 1f 67   ....M...I..D,-.g
0010 : 6c e5 05 a5 88 12 6b 8f a8 d3 e5 9e e0 55 e0 bd   l.....k......U..
0020 : 99 24 dd dc 72 36 8c c7 18 f5 69 00 00 22 00 39   .$..r6....i..".9
0030 : 00 38 00 37 00 36 00 35 00 33 00 32 00 31 00 30   .8.7.6.5.3.2.1.0
0040 : 00 2f 00 05 00 04 00 13 00 0d 00 16 00 10 00 0a   ./..............
0050 : 01 00                                             ..

 S: received 14 bytes (Alert messages 10 Unexpected message
    and Close Notify)
0000 : 15 03 00 00 02 02 0a 15 03 00 00 02 01 00         ..............
```

A.1.2. Successful connection

This example shows a TLS 1.0 Client Hello in a SSL v3.0 record, and the server responds with a Server Hello


```
 C : sending 82 bytes (Client Hello)
0000 : 16 03 00 00 4d 01 00 00 49 03 01 44 2c 35 2d 17   ....M...I..D,5-.
0010 : ad 60 c8 4d 8a 51 a5 59 f9 cd bc 3e b1 9c a2 ff   .`.M.Q.Y...>....
0020 : 42 71 33 2f 80 86 3f 4b f6 62 ea 00 00 22 00 39   Bq3/...K.b..."..9
0030 : 00 38 00 37 00 36 00 35 00 33 00 32 00 31 00 30   .8.7.6.5.3.2.1.0
0040 : 00 2f 00 05 00 04 00 13 00 0d 00 16 00 10 00 0a   ./..............
0050 : 01 00                                             ..

 S : received 47 bytes (Server Hello, v3.0)
0000 : 16 03 00 00 2a 02 00 00 26 03 00 44 2c 35 96 1d   ....*...&..D,5..
0010 : d5 02 df 00 eb 5d fb 32 2e 51 64 42 99 c4 94 c2   .....].2.QdB....
0020 : 46 61 b3 19 e1 50 28 93 57 a9 e9 00 00 05 00      Fa...P(.W......
```

A.1.3. Successful Connection

This example shows a SSL v2 Client Hello requesting a TLS 1.0 connection. The server responds with a SSL v3 Server Hello

```
 C : sending 138 bytes (SSL v2 Client Hello)
0000 : 80 88 01 03 01 00 6f 00 00 00 10 00 00 39 00 00   ......o......9..
0010 : 38 00 00 37 00 00 36 00 00 35 00 00 33 00 00 32   8..7..6..5..3..2
0020 : 00 00 31 00 00 30 00 00 2f 00 00 05 00 00 04 00   ..1..0../.......
0030 : 00 13 00 00 0d 00 00 16 00 00 10 00 00 0a 00 00   ................
0040 : 12 00 00 0c 00 00 15 00 00 0f 00 00 09 00 00 64   ...............d
0050 : 00 00 62 00 00 11 00 00 0b 00 00 14 00 00 0e 00   ..b.............
0060 : 00 08 00 00 03 00 00 06 01 00 80 07 00 c0 03 00   ................
0070 : 80 06 00 40 02 00 80 04 00 80 44 2c 36 28 d6 0e   ...@......D,6(..
0080 : d9 20 b8 9c d6 0f ad aa 80 d7                     . ........

 S : received 47 bytes (SSL v3 Server Hello)
0000 : 16 03 00 00 2a 02 00 00 26 03 00 44 2c 36 92 97   ....*...&..D,6..
0010 : 91 4f 1d b2 e1 96 e2 5c 99 c2 5c 21 8e 91 67 91   .O.....\..\!..g.
0020 : 4b 34 ee e7 78 56 65 7b 7a f0 ad 00 00 05 00      K4..xVe{z......
```

A.2. SSL v3 server refuses TLS 1.0 client (case 2)

Date: April 5, 2006

Server: Lotus-Domino/5.0.8

Site: https://www.ecbanking.com.my/

This site refused to connect with any client presenting the TLS 1.0 version number in the Client Hello message

A.2.1. Failed connection

This example uses an SSL v2 Client Hello, requesting a TLS 1.0 connection. The server closes the connection without sending any data or error messages to the client.

```
 C : Sending 138 bytes (SSL v2 Client Hello, requesting TLS 1.0)
0000 : 80 88 01 03 01 00 6f 00 00 00 10 00 00 39 00 00   ......o......9..
0010 : 38 00 00 37 00 00 36 00 00 35 00 00 33 00 00 32   8..7..6..5..3..2
0020 : 00 00 31 00 00 30 00 00 2f 00 00 05 00 00 04 00   ..1..0../.......
0030 : 00 13 00 00 0d 00 00 16 00 00 10 00 00 0a 00 00   ................
```

```
0040 : 12 00 00 0c 00 00 15 00 00 0f 00 00 09 00 00 64   ...............d
0050 : 00 00 62 00 00 11 00 00 0b 00 00 14 00 00 0e 00   ..b.............
0060 : 00 08 00 00 03 00 00 06 01 00 80 07 00 c0 03 00   ................
0070 : 80 06 00 40 02 00 80 04 00 80 44 33 0c 61 ef 3e   ...@......D3.a.>
0080 : 2f 10 6b 09 94 56 cc 7d 5c 18                     /.k..V.}\.

<S: close  of connection>
```

A.2.2. Successful connection

This example uses an SSL v2 Client Hello, requesting a SSL v3.0 connection. The server responds with a SSL v3.0 Server Hello

```
 C: Sending 138 bytes (SSL v2 Client Hello, requesting SSL v3.0)
0000 : 80 88 01 03 00 00 6f 00 00 00 10 00 00 39 00 00   ......o......9..
0010 : 38 00 00 37 00 00 36 00 00 35 00 00 33 00 00 32   8..7..6..5..3..2
0020 : 00 00 31 00 00 30 00 00 2f 00 00 05 00 00 04 00   ..1..0../.......
0030 : 00 13 00 00 0d 00 00 16 00 00 10 00 00 0a 00 00   ................
0040 : 12 00 00 0c 00 00 15 00 00 0f 00 00 09 00 00 64   ...............d
0050 : 00 00 62 00 00 11 00 00 0b 00 00 14 00 00 0e 00   ..b.............
0060 : 00 08 00 00 03 00 00 06 01 00 80 07 00 c0 03 00   ................
0070 : 80 06 00 40 02 00 80 04 00 80 44 33 0c 65 18 21   ...@......D3.e.!
0080 : bb 61 ee 4f 1b 7e 16 98 b2 2f                     .a.O.~.../

 S : Received 2560 bytes (SSL v3.0 Server Hello)
0000 : 16 03 00 0b 16 02 00 00 46 03 00 31 05 8d 10 01   ........F..1....
0010 : 5c 9c 2b f1 88 e8 e4 fa 42 0c 1a ff 95 df 49 a8   \.+.....B.....I.
0020 : a9 3d 74 35 fe 07 9d b3 6f 61 28 20 09 c3 e4 4e   .=t5....oa( ...N
0030 : e6 27 d1 90 11 55 19 ec 18 37 92 50 0d af 35 3b   .'...U...7.P..5;
0040 : 08 96 0f 53 32 67 e4 65 9e 75 19 62 00 05 00      ...S2g.e.u.b...
```

A.2.3. Failed connection

This example uses an TLS 1.0 Client Hello in a SSL v3.0 record, requesting a TLS 1.0 connection. The server responds with a Unexpected Message alert message


```
 C : Sending 110 bytes (TLS 1.0 Client Hello in SSL v3 record)
0000 : 16 03 00 00 69 01 00 00 65 03 01 44 33 16 76 4f   ....i...e..D3.vO
0010 : 90 61 33 15 6a 75 02 2c 23 70 7e f8 03 67 41 c8   .a3.ju.,#p~..gA.
0020 : 1d 30 22 5b ed be 8c 66 d3 bd 66 00 00 3e 00 39   .0"[...f..f..>.9
```

```
0030 : 00 38 00 37 00 36 00 35 00 33 00 32 00 31 00 30   .8.7.6.5.3.2.1.0
0040 : 00 2f 00 05 00 04 00 13 00 0d 00 16 00 10 00 0a   ./..............
0050 : 00 12 00 0c 00 15 00 0f 00 09 00 64 00 62 00 11   ...........d.b..
0060 : 00 0b 00 14 00 0e 00 08 00 03 00 06 01 00         ..............

 S : Received 7 bytes
0000 : 15 03 00 00 02 02 0a                              .......
```

A.2.4. Successful connection

This example uses an SSL v3 Client Hello, requesting a SSL v3.0 connection. The server responds with a SSL v3.0 Server Hello

```
 C : Sending 110 bytes (SSL v3 Client Hello)
0000 : 16 03 00 00 69 01 00 00 65 03 00 44 33 16 77 4b   ....i...e..D3.wK
0010 : fb 0a 6e d5 55 a7 45 86 95 16 01 a7 d2 c9 45 2c   ..n.U.E.......E,
0020 : 42 98 7e 71 59 87 03 72 6f d4 95 00 00 3e 00 39   B.~qY..ro....>.9
0030 : 00 38 00 37 00 36 00 35 00 33 00 32 00 31 00 30   .8.7.6.5.3.2.1.0
0040 : 00 2f 00 05 00 04 00 13 00 0d 00 16 00 10 00 0a   ./..............
0050 : 00 12 00 0c 00 15 00 0f 00 09 00 64 00 62 00 11   ...........d.b..
0060 : 00 0b 00 14 00 0e 00 08 00 03 00 06 01 00         ..............

 S : Received 2560 bytes (SSL v3 Server Hello)
0000 : 16 03 00 0b 16 02 00 00 46 03 00 30 e5 3f e0 52   ........F..0...R
0010 : f1 6a ae 5a a2 5b 51 5e 47 72 3d fa b4 10 0b 80   .j.Z.[Q^Gr=.....
0020 : 8a e1 ee e9 fa bc 72 67 cc 1e d2 20 7c 3b 3d 41   ......rg... |;=A
0030 : 80 77 d2 9f ca 73 81 b8 20 99 97 26 da 52 07 d3   .w...s.. ..&.R..
0040 : df f1 73 c9 14 e2 98 45 9a d2 e1 4c 00 05 00      ..s....E...L...
```

A.3. TLS 1.0 server refuses TLS 1.1 client

Date: April 25, 2006

Gateway: WebSphere

Site: https://www.dnbnor.no/

Highest supported version: TLS 1.0

This TLS 1.0 server shuts down the connection when it gets a connection request from a TLS 1.1 client.

According to information provided in private communications with the system administrators this site uses a Lotus Domino WebSphere server as a front-end, and that is where the connection is cut.

A.3.1. SSL v2 Client Hello

This example uses an SSL v2 Client Hello to request a TLS 1.1 connection, but the server immediately closes the connection without any error message.

```
 C: Sending 138 bytes (SSL v2 Client Hello, TLS 1.1 version requested)
0000 : 80 88 01 03 02 00 6f 00 00 00 10 00 00 39 00 00   ......o......9..
0010 : 38 00 00 37 00 00 36 00 00 35 00 00 33 00 00 32   8..7..6..5..3..2
0020 : 00 00 31 00 00 30 00 00 2f 00 00 05 00 00 04 00   ..1..0../.......
0030 : 00 13 00 00 0d 00 00 16 00 00 10 00 00 0a 00 00   ................
0040 : 12 00 00 0c 00 00 15 00 00 0f 00 00 09 00 00 64   ...............d
0050 : 00 00 62 00 00 11 00 00 0b 00 00 14 00 00 0e 00   ..b.............
0060 : 00 08 00 00 03 00 00 06 01 00 80 07 00 c0 03 00   ................
0070 : 80 06 00 40 02 00 80 04 00 80 44 4e 53 a8 24 1b   ...@......DNS.$.
0080 : 29 8f 20 17 27 74 46 24 f4 d1                     ). .'tF$..

<S: Connection shutdown>
```

A.3.2. TLS 1.0 Record, TLS 1.1 Client Hello

This example uses a TLS 1.0 Client Hello in a TLS 1.0 Record to request a TLS 1.1 connection, but the server immediately closes the connection without any error message.

```
 C: 82 bytes
0000 : 16 03 01 00 4d 01 00 00 49 03 02 44 4e 54 c4 e8   ....M...I..DNT..
0010 : 59 f9 9a e4 35 27 4f 95 b0 4b 82 4a 01 71 ea 8e   Y...5'O..K.J.q..
0020 : c0 29 2d 8e 8e f2 07 81 3d f6 4e 00 00 22 00 39   .)-.....=.N..".9
0030 : 00 38 00 37 00 36 00 35 00 33 00 32 00 31 00 30   .8.7.6.5.3.2.1.0
0040 : 00 2f 00 05 00 04 00 13 00 0d 00 16 00 10 00 0a   ./..............
0050 : 01 00                                             ..

<S: connection shutdown>
```

A.4. TLS 1.0 server refuses TLS Extensions

Date: April 25, 2006

Gateway: WebSphere

Site: https://www.dnbnor.no/

Highest supported version: TLS 1.0

This server (the same as in Appendix A.3) shuts down the connection when it gets a connection request from a TLS 1.0 client with support

for TLS Extensions.

According to information provided in private communications with the system administrators this site uses a Lotus Domino WebSphere server as a front-end, and that is where the connection is cut.

A.4.1. TLS 1.0 with TLS Extensions

This example uses a TLS 1.0 Client Hello with a ServerName and a Certificate Status TLS Extension in a TLS 1.0 Record to request a TLS 1.0 connection, but the server immediately closes the connection without any error message.

C: 150 bytes (TLS 1.0 Client Hello, with ServerName and Certificate Status TLS Extensions.

```
0000 : 16 03 01 00 91 01 00 00 8d 03 01 44 4e 54 c4 90   ...........DNT..
0010 : 98 a6 83 92 36 a8 79 6c a3 3f f8 dd 78 74 5b 7e   ....6.yl....xt[~
0020 : 8d fa a7 7d 1f ef 60 1e 99 bb 29 00 00 22 00 39   ...}..`...)..".9
0030 : 00 38 00 37 00 36 00 35 00 33 00 32 00 31 00 30   .8.7.6.5.3.2.1.0
0040 : 00 2f 00 05 00 04 00 13 00 0d 00 16 00 10 00 0a   ./..............
0050 : 01 00 00 42 00 00 00 12 00 10 00 00 0d 77 77 77   ...B.........www
0060 : 2e 64 6e 62 6e 6f 72 2e 6e 6f 00 05 00 28 01 00   .dnbnor.no...(..
0070 : 00 00 23 22 21 30 1f 06 09 2b 06 01 05 05 07 30   ..#"!0...+.....0
0080 : 01 02 04 12 04 10 64 7c 47 2d a1 b1 cb ab ca 36   ......d|G-.....6
0090 : d4 9e a6 64 92 e0                                 ...d..
```

<S: connection shutdown>

A.5. Renegotiation with SSL v3 records over TLS 1.0 connection

Date: June 5, 2006

Gateway: WebSphere

Site: https://www.dnbnor.no/

Highest supported version: TLS 1.0

This example was created using a specially modified TLS Client that immediately initiate a renegotiation of the TLS session, but does so using SSL v3 as the record protocol version, even over a TLS 1.0 negotiated encrypted connection. This is based on actual

observations of a client the author is not associated with.

When the renegotiation starts the server responds with an SSL v2 error code, not an SSL v3 or TLS 1.0 error code. At least one other server has been observed throwing TLS errors, as expected, but apparently a number of servers actually accept the type of negotiation performed in this case

According to information provided in private communications with the system administrators this site uses a Lotus Domino WebSphere server as a front-end, and that is where the connection is cut.

```
C : Sending 82 bytes (Client Hello requesting TLS 1.0 in a
    SSL v3.0  Record)
0000 : 16 03 00 00 4d 01 00 00 49 03 01 44 84 9f de 7c   ....M...I..D...|
0010 : f8 51 49 35 31 0a 0e d8 e1 a8 dc 97 dc 1b 22 b5   .QI51.........".
0020 : 96 96 c1 69 7b 5a 34 83 07 0d 5e 00 00 22 00 39   ...i{Z4...^..".9
0030 : 00 38 00 37 00 36 00 35 00 33 00 32 00 31 00 30   .8.7.6.5.3.2.1.0
0040 : 00 2f 00 05 00 04 00 13 00 0d 00 16 00 10 00 0a   ./..............
0050 : 01 00                                             ..

S : Received 2520 bytes (Server Hello TLS 1.0)
0000 : 16 03 01 0a 99 02 00 00 46 03 01 00 00 00 44 5c   ........F.....D\
0010 : 1d 7d 6a df 62 f0 f4 4c 74 f7 e5 df 31 e6 d2 43   .}j.b..Lt...1..C
0020 : 14 ee 56 9a 48 e9 90 97 56 b6 c6 20 00 00 51 c7   ..V.H...V.. ..Q.
0030 : 87 47 cd 99 56 93 d3 c5 1b f1 86 bb 19 88 59 e9   .G..V.........Y.
0040 : 58 58 58 58 44 84 9f e5 00 02 9b ae 00 35 00      XXXXD........5.

    (Certificate Part 1)
0040 :                                                  0b                .
0050 : 00 0a 47 00 0a 44 00 04 74 30 82 04 70 30 82 03   ..G..D..t0..p0..
0060 : d9 a0 03 02 01 02 02 10 77 f1 5a 9c af fb 1f 6b   ........w.Z....k
0070 : 38 2c 96 5b 53 7b ce aa 30 0d 06 09 2a 86 48 86   8,.[S{..0...*.H.
0080 : f7 0d 01 01 05 05 00 30 81 ba 31 1f 30 1d 06 03   .......0..1.0...
0090 : 55 04 0a 13 16 56 65 72 69 53 69 67 6e 20 54 72   U....VeriSign Tr
00a0 : 75 73 74 20 4e 65 74 77 6f 72 6b 31 17 30 15 06   ust Network1.0..
00b0 : 03 55 04 0b 13 0e 56 65 72 69 53 69 67 6e 2c 20   .U....VeriSign,
00c0 : 49 6e 63 2e 31 33 30 31 06 03 55 04 0b 13 2a 56   Inc.1301..U...*V
00d0 : 65 72 69 53 69 67 6e 20 49 6e 74 65 72 6e 61 74   eriSign Internat
00e0 : 69 6f 6e 61 6c 20 53 65 72 76 65 72 20 43 41 20   ional Server CA
00f0 : 2d 20 43 6c 61 73 73 20 33 31 49 30 47 06 03 55   - Class 31I0G..U
```

```
0100 : 04 0b 13 40 77 77 77 2e 76 65 72 69 73 69 67 6e   ...@www.verisign
0110 : 2e 63 6f 6d 2f 43 50 53 20 49 6e 63 6f 72 70 2e   .com/CPS Incorp.
0120 : 62 79 20 52 65 66 2e 20 4c 49 41 42 49 4c 49 54   by Ref. LIABILIT
0130 : 59 20 4c 54 44 2e 28 63 29 39 37 20 56 65 72 69   Y LTD.(c)97 Veri
0140 : 53 69 67 6e 30 1e 17 0d 30 35 30 39 30 35 30 30   Sign0...05090500
0150 : 30 30 30 30 5a 17 0d 30 37 30 39 30 35 32 33 35   0000Z..070905235
0160 : 39 35 39 5a 30 81 a8 31 0b 30 09 06 03 55 04 06   959Z0..1.0...U..
0170 : 13 02 4e 4f 31 0f 30 0d 06 03 55 04 08 13 06 42   ..NO1.0...U....B
0180 : 65 72 67 65 6e 31 10 30 0e 06 03 55 04 07 14 07   ergen1.0...U....
0190 : 53 61 6e 64 73 6c 69 31 15 30 13 06 03 55 04 0a   Sandsli1.0...U..
01a0 : 14 0c 45 44 42 20 49 54 20 44 72 69 66 74 31 12   ..EDB IT Drift1.
01b0 : 30 10 06 03 55 04 0b 14 09 44 6e 42 4e 4f 52 20   0...U....DnBNOR
01c0 : 49 54 31 33 30 31 06 03 55 04 0b 14 2a 54 65 72   IT1301..U...*Ter
01d0 : 6d 73 20 6f 66 20 75 73 65 20 61 74 20 77 77 77   ms of use at www
01e0 : 2e 76 65 72 69 73 69 67 6e 2e 63 6f 6d 2f 72 70   .verisign.com/rp
```



```
01f0 : 61 20 28 63 29 30 30 31 16 30 14 06 03 55 04 03   a (c)001.0...U..
0200 : 14 0d 77 77 77 2e 64 6e 62 6e 6f 72 2e 6e 6f 30   ..www.dnbnor.no0
0210 : 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05   ..0...*.H.......
0220 : 00 03 81 8d 00 30 81 89 02 81 81 00 b5 b5 b1 17   .....0..........
0230 : 6d c0 e4 78 64 7d 89 7d e9 fa 62 1b 6b 59 d4 39   m..xd}.}..b.kY.9
0240 : 8e 5a 78 d5 50 2b 5a 3d c7 5b 02 87 df 67 51 0f   .Zx.P+Z=.[...gQ.
0250 : b2 d9 43 6e 00 33 c3 88 fb 4e ac 31 85 82 ca a6   ..Cn.3...N.1....
0260 : 96 84 9c 99 64 fa 44 b6 c5 3e 87 bb 81 72 25 b0   ....d.D..>...r%.
0270 : de a5 27 5d 9d 17 e5 c7 73 6a 08 7e 90 c4 b9 e2   ..']....sj.~....
0280 : 78 f1 70 b5 06 44 4d 4d 60 fa e8 b8 a0 6b 04 11   x.p..DMM`....k..
0290 : 7e 4e f2 61 79 57 ad 0f a1 2d b8 b5 1b ea d2 a5   ~N.ayW...-......
02a0 : 96 28 53 cc 6b f8 f1 4c 15 5b 4b 17 02 03 01 00   .(S.k..L.[K.....
02b0 : 01 a3 82 01 85 30 82 01 81 30 09 06 03 55 1d 13   .....0...0...U..
02c0 : 04 02 30 00 30 0b 06 03 55 1d 0f 04 04 03 02 05   ..0.0...U.......
02d0 : a0 30 46 06 03 55 1d 1f 04 3f 30 3d 30 3b a0 39   .0F..U....0=0;.9
02e0 : a0 37 86 35 68 74 74 70 3a 2f 2f 63 72 6c 2e 76   .7.5http://crl.v
02f0 : 65 72 69 73 69 67 6e 2e 63 6f 6d 2f 43 6c 61 73   erisign.com/Clas
0300 : 73 33 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 53   s3InternationalS
0310 : 65 72 76 65 72 2e 63 72 6c 30 44 06 03 55 1d 20   erver.crl0D..U.
0320 : 04 3d 30 3b 30 39 06 0b 60 86 48 01 86 f8 45 01   .=0;09..`.H...E.
0330 : 07 17 03 30 2a 30 28 06 08 2b 06 01 05 05 07 02   ...0*0(..+......
0340 : 01 16 1c 68 74 74 70 73 3a 2f 2f 77 77 77 2e 76   ...https://www.v
0350 : 65 72 69 73 69 67 6e 2e 63 6f 6d 2f 72 70 61 30   erisign.com/rpa0
0360 : 34 06 03 55 1d 25 04 2d 30 2b 06 09 60 86 48 01   4..U.%.-0+..`.H.
0370 : 86 f8 42 04 01 06 0a 2b 06 01 04 01 82 37 0a 03   ..B....+.....7..
0380 : 03 06 08 2b 06 01 05 05 07 03 01 06 08 2b 06 01   ...+.........+..
```

```
0390 : 05 05 07 03 02 30 34 06 08 2b 06 01 05 05 07 01   .....04..+......
03a0 : 01 04 28 30 26 30 24 06 08 2b 06 01 05 05 07 30   ..(0&0$..+.....0
03b0 : 01 86 18 68 74 74 70 3a 2f 2f 6f 63 73 70 2e 76   ...http://ocsp.v
03c0 : 65 72 69 73 69 67 6e 2e 63 6f 6d 30 6d 06 08 2b   erisign.com0m..+
03d0 : 06 01 05 05 07 01 0c 04 61 30 5f a1 5d a0 5b 30   ........a0_.].[0
03e0 : 59 30 57 30 55 16 09 69 6d 61 67 65 2f 67 69 66   Y0W0U..image/gif
03f0 : 30 21 30 1f 30 07 06 05 2b 0e 03 02 1a 04 14 8f   0!0.0...+.......
0400 : e5 d3 1a 86 ac 8d 8e 6b c3 cf 80 6a d4 48 18 2c   .......k...j.H.,
0410 : 7b 19 2e 30 25 16 23 68 74 74 70 3a 2f 2f 6c 6f   {..0%.#http://lo
0420 : 67 6f 2e 76 65 72 69 73 69 67 6e 2e 63 6f 6d 2f   go.verisign.com/
0430 : 76 73 6c 6f 67 6f 2e 67 69 66 30 0d 06 09 2a 86   vslogo.gif0...*.
0440 : 48 86 f7 0d 01 01 05 05 00 03 81 81 00 45 bc 3c   H............E.<
0450 : a1 80 f8 f9 30 d4 97 09 dd 21 22 55 13 b1 a7 fd   ....0....!"U....
0460 : b2 c4 7a 13 6a 65 7d 86 f1 5f ec 9a 27 e3 bf da   ..z.je}.._..'...
0470 : 0c e7 cc 64 cd b5 21 0e d1 5e 77 80 8f 73 6c b0   ...d..!..^w..sl.
0480 : 1b d9 1b 70 e2 c5 46 22 0a d3 c5 9e 42 6e 16 20   ...p..F"....Bn.
0490 : 43 e7 c3 a2 7c 9c 7a c0 f5 be c3 d5 a5 4f 3e 78   C...|.z......O>x
04a0 : 2d f8 ac 7c 8f 05 73 66 cb 81 a0 42 28 f8 06 01   -..|..sf...B(...
04b0 : 3a b5 8c 6c 34 1e d0 61 58 43 25 e0 fc d1 46 4d   :..l4..aXC%...FM
04c0 : 7e 1b 36 23 03 bb d6 4d 61 d8 d7 aa 05 00 03 87   ~.6#...Ma.......
04d0 : 30 82 03 83 30 82 02 ec a0 03 02 01 02 02 10 25   0...0..........%
04e0 : 4b 8a 85 38 42 cc e3 58 f8 c5 dd ae 22 6e a4 30   K..8B..X...."n.0
```



```
04f0 : 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00 30 5f   ...*.H........0_
0500 : 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 17 30   1.0...U....US1.0
0510 : 15 06 03 55 04 0a 13 0e 56 65 72 69 53 69 67 6e   ...U....VeriSign
0520 : 2c 20 49 6e 63 2e 31 37 30 35 06 03 55 04 0b 13   , Inc.1705..U...
0530 : 2e 43 6c 61 73 73 20 33 20 50 75 62 6c 69 63 20   .Class 3 Public
0540 : 50 72 69 6d 61 72 79 20 43 65 72 74 69 66 69 63   Primary Certific
0550 : 61 74 69 6f 6e 20 41 75 74 68 6f 72 69 74 79 30   ation Authority0
0560 : 1e 17 0d 39 37 30 34 31 37 30 30 30 30 30 30 5a   ...970417000000Z
0570 : 17 0d 31 31 31 30 32 34 32 33 35 39 35 39 5a 30   ..111024235959Z0
0580 : 81 ba 31 1f 30 1d 06 03 55 04 0a 13 16 56 65 72   ..1.0...U....Ver
0590 : 69 53 69 67 6e 20 54 72 75 73 74 20 4e 65 74 77   iSign Trust Netw
05a0 : 6f 72 6b 31 17 30 15 06 03 55 04 0b 13 0e 56 65   ork1.0...U....Ve
05b0 : 72 69 53 69 67 6e 2c 20 49 6e 63 2e 31 33 30 31   riSign, Inc.1301
05c0 : 06 03 55 04 0b 13 2a 56 65 72 69 53 69 67 6e 20   ..U...*VeriSign
05d0 : 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 20 53 65   International Se
05e0 : 72 76 65 72 20 43 41 20 2d 20 43 6c 61 73 73 20   rver CA - Class
05f0 : 33 31 49 30 47 06 03 55 04 0b 13 40 77 77 77 2e   31I0G..U...@www.
0600 : 76 65 72 69 73 69 67 6e 2e 63 6f 6d 2f 43 50 53   verisign.com/CPS
0610 : 20 49 6e 63 6f 72 70 2e 62 79 20 52 65 66 2e 20    Incorp.by Ref.
```

```
0620 : 4c 49 41 42 49 4c 49 54 59 20 4c 54 44 2e 28 63   LIABILITY LTD.(c
0630 : 29 39 37 20 56 65 72 69 53 69 67 6e 30 81 9f 30   )97 VeriSign0..0
0640 : 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 81   ...*.H..........
0650 : 8d 00 30 81 89 02 81 81 00 d8 82 80 e8 d6 19 02   ..0.............
0660 : 7d 1f 85 18 39 25 a2 65 2b e1 bf d4 05 d3 bc e6   }...9%.e+.......
0670 : 36 3b aa f0 4c 6c 5b b6 e7 aa 3c 73 45 55 b2 f1   6;..Ll[...<sEU..
0680 : bd ea 97 42 ed 9a 34 0a 15 d4 a9 5c f5 40 25 dd   ...B..4....\.@%.
0690 : d9 07 c1 32 b2 75 6c c4 ca bb a3 fe 56 27 71 43   ...2.ul.....V'qC
06a0 : aa 63 f5 30 3e 93 28 e5 fa f1 09 3b f3 b7 4d 4e   .c.0>.(....;..MN
06b0 : 39 f7 5c 49 5a b8 c1 1d d3 b2 8a fe 70 30 95 42   9.\IZ.......p0.B
06c0 : cb fe 2b 51 8b 5a 3c 3a f9 22 4f 90 b2 02 a7 53   ..+Q.Z<:."O....S
06d0 : 9c 4f 34 e7 ab 04 b2 7b 6f 02 03 01 00 01 a3 81   .O4....{o.......
06e0 : e3 30 81 e0 30 0f 06 03 55 1d 13 04 08 30 06 01   .0..0...U....0..
06f0 : 01 ff 02 01 00 30 44 06 03 55 1d 20 04 3d 30 3b   .....0D..U. .=0;
0700 : 30 39 06 0b 60 86 48 01 86 f8 45 01 07 01 01 30   09..`.H...E....0
0710 : 2a 30 28 06 08 2b 06 01 05 05 07 02 01 16 1c 68   *0(..+.........h
0720 : 74 74 70 73 3a 2f 2f 77 77 77 2e 76 65 72 69 73   ttps://www.veris
0730 : 69 67 6e 2e 63 6f 6d 2f 43 50 53 30 34 06 03 55   ign.com/CPS04..U
0740 : 1d 25 04 2d 30 2b 06 08 2b 06 01 05 05 07 03 01   .%.-0+..+.......
0750 : 06 08 2b 06 01 05 05 07 03 02 06 09 60 86 48 01   ..+.........`.H.
0760 : 86 f8 42 04 01 06 0a 60 86 48 01 86 f8 45 01 08   ..B....`.H...E..
0770 : 01 30 0b 06 03 55 1d 0f 04 04 03 02 01 06 30 11   .0...U........0.
0780 : 06 09 60 86 48 01 86 f8 42 01 01 04 04 03 02 01   ..`.H...B.......
0790 : 06 30 31 06 03 55 1d 1f 04 2a 30 28 30 26 a0 24   .01..U...*0(0&.$
07a0 : a0 22 86 20 68 74 74 70 3a 2f 2f 63 72 6c 2e 76   ." http://crl.v
07b0 : 65 72 69 73 69 67 6e 2e 63 6f 6d 2f 70 63 61 33   erisign.com/pca3
07c0 : 2e 63 72 6c 30 0d 06 09 2a 86 48 86 f7 0d 01 01   .crl0...*.H.....
07d0 : 05 05 00 03 81 81 00 08 01 ec e4 68 94 03 42 f1   ...........h..B.
07e0 : 73 f1 23 a2 3a de e9 f1 da c6 54 c4 23 3e 86 ea   s.#.:.....T.#>..
```



```
07f0 : cf 6a 3a 33 ab ea 9c 04 14 07 36 06 0b f9 88 6f   .j:3......6....o
0800 : d5 13 ee 29 2b c3 e4 72 8d 44 ed d1 ac 20 09 2d   ...)+..r.D... .-
0810 : e1 f6 e1 19 05 38 b0 3d 0f 9f 7f f8 9e 02 dc 86   .....8.=........
0820 : 02 86 61 4e 26 5f 5e 9f 92 1e 0c 24 a4 f5 d0 70   ..aN&_^....$...p
0830 : 13 cf 26 c3 43 3d 49 1d 9e 82 2e 52 5f bc 3e c6   ..&.C=I....R_.>.
0840 : 66 29 01 8e 4e 92 2c bc 46 75 03 82 ac 73 e9 d9   f)..N.,.Fu...s..
0850 : 7e 0b 67 ef 54 52 1a 00 02 40 30 82 02 3c 30 82   ~.g.TR...@0..<0.
0860 : 01 a5 02 10 70 ba e4 1d 10 d9 29 34 b6 38 ca 7b   ....p.....)4.8.{
0870 : 03 cc ba bf 30 0d 06 09 2a 86 48 86 f7 0d 01 01   ....0...*.H.....
0880 : 02 05 00 30 5f 31 0b 30 09 06 03 55 04 06 13 02   ...0_1.0...U....
0890 : 55 53 31 17 30 15 06 03 55 04 0a 13 0e 56 65 72   US1.0...U....Ver
08a0 : 69 53 69 67 6e 2c 20 49 6e 63 2e 31 37 30 35 06   iSign, Inc.1705.
```

```
08b0 : 03 55 04 0b 13 2e 43 6c 61 73 73 20 33 20 50 75   .U....Class 3 Pu
08c0 : 62 6c 69 63 20 50 72 69 6d 61 72 79 20 43 65 72   blic Primary Cer
08d0 : 74 69 66 69 63 61 74 69 6f 6e 20 41 75 74 68 6f   tification Autho
08e0 : 72 69 74 79 30 1e 17 0d 39 36 30 31 32 39 30 30   rity0...96012900
08f0 : 30 30 30 30 5a 17 0d 32 38 30 38 30 31 32 33 35   0000Z..280801235
0900 : 39 35 39 5a 30 5f 31 0b 30 09 06 03 55 04 06 13   959Z0_1.0...U...
0910 : 02 55 53 31 17 30 15 06 03 55 04 0a 13 0e 56 65   .US1.0...U....Ve
0920 : 72 69 53 69 67 6e 2c 20 49 6e 63 2e 31 37 30 35   riSign, Inc.1705
0930 : 06 03 55 04 0b 13 2e 43 6c 61 73 73 20 33 20 50   ..U....Class 3 P
0940 : 75 62 6c 69 63 20 50 72 69 6d 61 72 79 20 43 65   ublic Primary Ce
0950 : 72 74 69 66 69 63 61 74 69 6f 6e 20 41 75 74 68   rtification Auth
0960 : 6f 72 69 74 79 30 81 9f 30 0d 06 09 2a 86 48 86   ority0..0...*.H.
0970 : f7 0d 01 01 01 05 00 03 81 8d 00 30 81 89 02 81   ...........0....
0980 : 81 00 c9 5c 59 9e f2 1b 8a 01 14 b4 10 df 04 40   ...\Y..........@
0990 : db e3 57 af 6a 45 40 8f 84 0c 0b d1 33 d9 d9 11   ..W.jE@.....3...
09a0 : cf ee 02 58 1f 25 f7 2a a8 44 05 aa ec 03 1f 78   ...X.%.*.D.....x
09b0 : 7f 9e 93 b9 9a 00 aa 23 7d d6 ac 85 a2 63 45 c7   .......#}....cE.
09c0 : 72 27 cc f4 4c c6 75 71 d2 39 ef 4f 42 f0 75 df   r'..L.uq.9.OB.u.
09d0 : 0a 90 c6 8e 20 6f 98 0f                           .... o..

S : received 198 bytes (Certificate part 2)
0000 : f8 ac 23 5f 70 29 36 a4 c9 86 e7 b1 9a 20 cb 53   ..#_p)6..... .S
0010 : a5 85 e7 3d be 7d 9a fe 24 45 33 dc 76 15 ed 0f   ...=.}..$E3.v...
0020 : a2 71 64 4c 65 2e 81 68 45 a7 02 03 01 00 01 30   .qdLe..hE......0
0030 : 0d 06 09 2a 86 48 86 f7 0d 01 01 02 05 00 03 81   ...*.H..........
0040 : 81 00 bb 4c 12 2b cf 2c 26 00 4f 14 13 dd a6 fb   ...L.+.,&.O.....
0050 : fc 0a 11 84 8c f3 28 1c 67 92 2f 7c b6 c5 fa df   ......(.g./|....
0060 : f0 e8 95 bc 1d 8f 6c 2c a8 51 cc 73 d8 a4 c0 53   ......l,.Q.s...S
0070 : f0 4e d6 26 c0 76 01 57 81 92 5e 21 f1 d1 b1 ff   .N.&.v.W..^!....
0080 : e7 d0 21 58 cd 69 17 e3 44 1c 9c 19 44 39 89 5c   ..!X.i..D...D9.\
0090 : dc 9c 00 0f 56 8d 02 99 ed a2 90 45 4c e4 bb 10   ....V......EL...
00a0 : a4 3d f0 32 03 0e f1 ce f8 e8 c9 51 8c e6 62 9f   .=.2.......Q..b.
00b0 : e6 9f c0 7d b7 72 9c c9 36 3a 6b 9f 4e a8 ff 64   ...}.r..6:k.N..d
00c0 : 0d 64                                             .d
```

(Hello Done)


```
00c0 :       0e 00 00 00                                 ....
```

```
C : Sending 139 bytes (Client Key exchange)
0000 : 16 03 01 00 86 10 00 00 82 00 80 43 4b e5 84 c9   ...........CK...
```

```
0010 : 27 e9 b3 6b 04 d4 54 a7 33 83 70 9f e1 80 c5 24   '..k..T.3.p....$
0020 : fc 3e 9d fe 3d 11 64 14 64 f9 e2 30 68 1e 4d c6   .>..=.d.d..0h.M.
0030 : 2d 16 5f a0 25 1e 6a 51 cf 32 42 00 2c 5e e9 58   -._.%.jQ.2B.,^.X
0040 : cc 33 ad 2e 9b e9 6b 12 5c 23 ac b1 37 9b 4a 2b   .3....k.\#..7.J+
0050 : 28 f9 57 d9 92 89 01 f3 6b 94 a3 18 dc f6 1f e1   (.W.....k.......
0060 : f0 68 de 54 de f0 58 e3 7a 58 09 dd 3b 07 f7 df   .h.T..X.zX..;...
0070 : 5b 62 04 73 38 7c 6c 00 81 61 e7 85 a6 32 9d 45   [b.s8|l..a...2.E
0080 : 6b f4 34 00 7d cf d7 7b d0 3e da                  k.4.}..{.>.

C : Sending 6 bytes (Cipher Change)
0000 : 14 03 01 00 01 01                                 ......

C : Plaintext 16 bytes (Finished)
0000 : 14 00 00 0c 7c cf 8d 7b 62 76 ab 9a ae b6 e5 6e   ....|..{bv.....n

C : Sending 53 bytes (Encrypted Finished)
0000 : 16 03 01 00 30 6f fd 31 80 51 a9 3d 18 7d 55 ef   ....0o.1.Q.=.}U.
0010 : 7c 6c 80 07 b2 79 6a 06 39 79 7e 15 7d e8 ee 1f   |l...yj.9y~.}...
0020 : fd be 68 6a af e2 cd db 47 f9 a6 b8 20 26 b9 03   ..hj....G... &..
0030 : 12 ec d3 c3 fd                                    .....

S : Received 6 bytes  (Cipher Change)
0000 : 14 03 01 00 01 01                                 ......

S : Received 53 bytes  (Encrypted Finished)
0000 : 16 03 01 00 30 a4 11 4c 05 28 3b cc 39 d3 aa 63   ....0..L.(;.9..c
0010 : bc 9d 74 f8 9b 8e 1c 6b 5c ee f2 4b 82 e9 ce c9   ..t....k\..K....
0020 : ce 73 b9 28 c2 2d 84 92 a3 70 5b 5b a8 8b 4f 86   .s.(.-...p[[..O.
0030 : 59 90 bf 39 9f                                    Y..9.

S : Plaintext 16 bytes (Plaintext Finished)
0000 : 14 00 00 0c 78 40 33 0f ae eb f4 e4 19 bd e8 66   ....x@3........f

C : Plaintext 109 bytes (Client Hello requesting TLS 1.0)
0000 : 01 00 00 69 03 01 44 84 9f e0 38 4e 2b 3c 01 4d   ...i..D...8N+<.M
0010 : d2 9c c0 03 fd 1f 92 f4 b7 d2 27 61 9e 68 a2 bf   ..........'a.h..
0020 : 7d fc f2 98 5d d6 20 00 00 51 c7 87 47 cd 99 56   }...]. ..Q..G..V
0030 : 93 d3 c5 1b f1 86 bb 19 88 59 e9 58 58 58 58 44   .........Y.XXXXD
0040 : 84 9f e5 00 02 9b ae 00 22 00 35 00 39 00 38 00   ........".5.9.8.
0050 : 37 00 33 00 32 00 31 00 30 00 2f 00 05 00 04 00   7.3.2.1.0./.....
0060 : 13 00 0d 00 16 00 10 00 0a 00 00 01 00            .............

C : Sending 149 bytes (Encrypted Client Hello,
```

```
    SSL v3.0 record protocol over TLS 1.0 encrypted connection)
0000 : 16 03 00 00 90 d6 39 9d 73 59 a4 88 61 9d ea f6   ......9.sY..a...
0010 : 43 f0 96 12 86 5d 50 fb 81 8d e7 c5 7d 57 1b d5   C....]P.....}W..
0020 : a6 f7 24 a9 9d b0 a4 5c 93 60 c3 6a 8f d5 b5 1b   ..$....\.`.j....
0030 : e1 96 af 8f 2e 94 0a 69 05 0c e2 8c 0d c5 a5 31   .......i.......1
0040 : 6f 2b 41 77 8e e8 d3 8e 16 96 87 b7 3d 9d 83 1b   o+Aw........=...
0050 : 1e 04 15 27 80 8e 67 05 d3 ee 9f 82 63 13 10 a0   ...'..g.....c...
0060 : 29 70 ce c4 9e c0 22 94 15 39 d8 07 fd 88 0c bb   )p....".9......
0070 : ff 00 26 34 1f 63 f1 fc 36 5f 30 fe 51 ef f4 78   ..&4.c..6_0.Q..x
0080 : dd df f1 7b c2 91 f9 29 e4 e2 5c 1f 10 98 b8 c8   ...{...)..\.....
0090 : ec cc 13 d9 da                                    .....

S : Received 5 bytes (SSL v2 Error message)
0000 : 80 03 00 00 01                                    .....
```

A.6. Wrong version expected in RSA Client Key Exchange

Date: June 15, 2006

Server: Stronghold/2.4.2 Apache/1.3.6 C2NetEU/2412 (Unix)

Site: https://www.gotogate.no/

Highest supported version: TLS 1.0

This server negotiates a TLS 1.0 connection when TLS 1.1 is offered, but after receiving the RSA Client Key Exchange the server sends a handshake error and closes the connection, as seen in Appendix A.6.1. The reason for the error is that the server expects the negotiated version to be used in the Premaster Secret, not the version used in the Client Hello, as seen in Appendix A.6.2

A.6.1. Correct Premaster - Connection Failure

This is a normal TLS handshake requesting a TLS 1.1 connection from the server. The server selects TLS 1.0, but reports a handshake failure after the Client Key Exchange message has been sent.

```
C : Sending 82 bytes (Client Hello Requesting TLS 1.1,
    in a TLS 1.0 Record)
0000 : 16 03 01 00 4d 01 00 00 49 03 02 44 90 b9 63 a2   ....M...I..D..c.
0010 : 1b bd 07 1d 01 55 3f 8a 9e c9 0a a1 99 dc 8a 1b   .....U...?.?....
0020 : d8 62 dc 07 bc 0c 58 99 0c e0 a4 00 00 22 00 39   .b....X..?...".9
0030 : 00 38 00 37 00 36 00 35 00 33 00 32 00 31 00 30   .8.7.6.5.3.2.1.0
0040 : 00 2f 00 05 00 04 00 13 00 0d 00 16 00 10 00 0a   ./..............
0050 : 01 00                                             ..

S : Received 948 bytes (Server hello)
```

```
0000 : 16 03 01 00 4a 02 00 00 46 03 01 44 90 b8 cb 2f   ....J...F..D.??/
0010 : e2 a7 3e 22 f8 af 5d 62 ca ab c1 6a c1 16 5f 88   ?.>".?]b?.?j?._.
0020 : 64 81 5d 24 52 8b 2f 72 6d 97 c9 20 71 09 06 7d   d.]$R./rm.? q..}
0030 : 64 a4 8a ce e7 4c 4b bc 20 e5 db 5e 49 46 9d 51   d..??LK. .?^IF.Q
0040 : 01 bb f6 e1 4c e5 f6 0e bb b9 23 6f 00 05 00      ..........#o...

    (Certificate)
0040 :                                              16                .
0050 : 03 01 03 57 0b 00 03 53 00 03 50 00 03 4d 30 82   ...W...S..P..M0.
0060 : 03 49 30 82 02 b2 a0 03 02 01 02 02 03 3f 84 41   .I0...?........A
0070 : 30 0d 06 09 2a 86 48 86 f7 0d 01 01 04 05 00 30   0...*.H.?......0
0080 : 81 ce 31 0b 30 09 06 03 55 04 06 13 02 5a 41 31   .?1.0...U....ZA1
0090 : 15 30 13 06 03 55 04 08 13 0c 57 65 73 74 65 72   .0...U....Wester
00a0 : 6e 20 43 61 70 65 31 12 30 10 06 03 55 04 07 13   n Cape1.0...U...
00b0 : 09 43 61 70 65 20 54 6f 77 6e 31 1d 30 1b 06 03   .Cape Town1.0...
00c0 : 55 04 0a 13 14 54 68 61 77 74 65 20 43 6f 6e 73   U....Thawte Cons
00d0 : 75 6c 74 69 6e 67 20 63 63 31 28 30 26 06 03 55   ulting cc1(0&..U
00e0 : 04 0b 13 1f 43 65 72 74 69 66 69 63 61 74 69 6f   ....Certificatio
00f0 : 6e 20 53 65 72 76 69 63 65 73 20 44 69 76 69 73   n Services Divis
0100 : 69 6f 6e 31 21 30 1f 06 03 55 04 03 13 18 54 68   ion1!0...U....Th
0110 : 61 77 74 65 20 50 72 65 6d 69 75 6d 20 53 65 72   awte Premium Ser
0120 : 76 65 72 20 43 41 31 28 30 26 06 09 2a 86 48 86   ver CA1(0&..*.H.
0130 : f7 0d 01 09 01 16 19 70 72 65 6d 69 75 6d 2d 73   ?......premium-s
0140 : 65 72 76 65 72 40 74 68 61 77 74 65 2e 63 6f 6d   erver@thawte.com
0150 : 30 1e 17 0d 30 35 30 36 32 31 31 31 30 37 33 39   0...050621110739
0160 : 5a 17 0d 30 36 30 36 32 31 31 31 30 37 33 39 5a   Z..060621110739Z
0170 : 30 5b 31 0b 30 09 06 03 55 04 06 13 02 4e 4f 31   0[1.0...U....NO1
0180 : 0d 30 0b 06 03 55 04 08 13 04 4f 73 6c 6f 31 0d   .0...U....Oslo1.
0190 : 30 0b 06 03 55 04 07 13 04 4f 73 6c 6f 31 14 30   0...U....Oslo1.0
01a0 : 12 06 03 55 04 0a 13 0b 47 4f 54 4f 47 41 54 45   ...U....GOTOGATE
01b0 : 20 41 53 31 18 30 16 06 03 55 04 03 13 0f 77 77    AS1.0...U....ww
01c0 : 77 2e 67 6f 74 6f 67 61 74 65 2e 6e 6f 30 81 9f   w.gotogate.no0..
01d0 : 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03   0...*.H.?.......
01e0 : 81 8d 00 30 81 89 02 81 81 00 ca e1 b4 e6 2a cb   ...0......???.*?
01f0 : 27 c0 d3 17 d0 f8 8b 91 62 f9 97 84 86 b5 9e 0b   '??.....b?......
0200 : 1d df 97 b1 ce 7e 12 25 59 f2 80 d2 bf 8e 7b 56   .....?~.%Y?.??.{V
0210 : d0 cb 3c 1a ba c9 c6 0f 50 5b 17 b6 fd 66 ed c3   .?<.??..P[..?f??
0220 : 32 29 9b cd bb fd a4 9a 5a c1 67 48 2e 61 fa a6   2).?.?..Z?gH.a??
0230 : 48 1d ef 63 3c 97 38 6e a5 48 4c d8 e1 fe ec ec   H.?c<.8n.HL.?.??
0240 : ce 49 5a 86 54 43 ff 40 f2 8e 4c 26 35 d8 a3 19   ?IZ.TC?@?.L&5...
0250 : c6 e1 b9 6e ac 45 17 1d 37 32 85 18 d0 e3 41 d8   .?.n.E..72...?A.
0260 : c3 21 7b 67 e7 4f 37 64 f8 a9 02 03 01 00 01 a3   ?!{g?O7d........
```

```
0270 : 81 a6 30 81 a3 30 1d 06 03 55 1d 25 04 16 30 14   .?0..0...U.%..0.
0280 : 06 08 2b 06 01 05 05 07 03 01 06 08 2b 06 01 05   ..+.........+...
0290 : 05 07 03 02 30 40 06 03 55 1d 1f 04 39 30 37 30   ....0@..U...9070
02a0 : 35 a0 33 a0 31 86 2f 68 74 74 70 3a 2f 2f 63 72   5?3?1./http://cr
02b0 : 6c 2e 74 68 61 77 74 65 2e 63 6f 6d 2f 54 68 61   l.thawte.com/Tha
02c0 : 77 74 65 50 72 65 6d 69 75 6d 53 65 72 76 65 72   wtePremiumServer
```



```
02d0 : 43 41 2e 63 72 6c 30 32 06 08 2b 06 01 05 05 07   CA.crl02..+.....
02e0 : 01 01 04 26 30 24 30 22 06 08 2b 06 01 05 05 07   ...&0$0"..+.....
02f0 : 30 01 86 16 68 74 74 70 3a 2f 2f 6f 63 73 70 2e   0...http://ocsp.
0300 : 74 68 61 77 74 65 2e 63 6f 6d 30 0c 06 03 55 1d   thawte.com0...U.
0310 : 13 01 01 ff 04 02 30 00 30 0d 06 09 2a 86 48 86   ...?..0.0...*.H.
0320 : f7 0d 01 01 04 05 00 03 81 81 00 60 28 92 bc 07   ?..........`(...
0330 : 1f 96 76 d8 26 bd 10 59 8a 02 17 f3 a3 60 bc fc   ..v.&..Y...?.`..
0340 : 2a 4e b1 41 17 85 b3 b2 b0 4d db 43 d8 a4 f2 a9   *N.A....?M?C..?.
0350 : 7d 41 80 6d e7 fd ac 13 65 59 8c f3 81 6b 7c 0a   }A.m??..eY.?.k|.
0360 : b7 17 0d 00 4e 71 f4 84 f5 d2 30 b1 98 34 4b 2c   ?...Nq?.??0..4K,
0370 : b0 d0 0b 6d 85 e9 4d 6d 10 56 90 bd 36 b5 f3 5e   ?..m.?Mm.V..6.?^
0380 : ed 21 72 93 21 fc 90 d9 78 92 08 8b 6b b2 e9 0c   ?!r.!..?x...k.?.
0390 : 5a 19 54 b9 1a c9 ed c2 59 72 44 d3 13 57 08 15   Z.T..???YrD?.W..
03a0 : 1a 32 dd d9 53 23 85 76 d1 1c 0d 16 03 01 00 04   .2??S#.v?.......

    (Hello Done)
03b0 : 0e 00 00 00                                       ....

C : Plain Premaster Secret (correct version v3.2, from Client Hello)
0000 : 03 02 93 99 39 68 bc 45 f3 a0 d9 1e cd d5 bc 51   ....9h.E???.??.Q
0010 : 6b 79 b4 c5 c9 98 52 44 c0 57 ba 60 67 b3 bb dd   ky?.?.RD?W?`g..?
0020 : 05 56 e8 79 93 78 39 ba 44 27 7e 1d 07 46 6b 4d   .V?y.x9?D'~..FkM

C : Sending 139 bytes (Client Key Exchange)
0000 : 16 03 01 00 86 10 00 00 82 00 80 17 2c 16 c7 3b   ............,.?;
0010 : fc c9 29 da e1 21 37 c6 86 93 46 2c 94 1d b8 eb   .?)??!7...F,..??
0020 : 06 8a 78 05 80 af 60 5b 6b 73 fb c1 56 b4 8e 21   ..x..?`[ks??V?.!
0030 : 91 56 51 62 9d f0 b1 f6 28 45 5a 25 ab 7e 4e 1d   .VQb....(EZ%.~N.
0040 : 2c 93 e4 01 f5 3e df d3 31 5b 3e b8 41 95 21 95   ,...?>.?1[>?A.!.
0050 : e5 c4 d0 5b 6f 12 36 eb c8 44 8f 16 cf a3 9a c8   ...[o.6??D..?..?
0060 : 8a 70 bc 60 b2 ca 1d d3 1b 8b d3 49 4f 0a 72 d7   .p.`.?.?..?IO.r?
0070 : ca 87 99 1b 73 4d 1b 32 bc ed 9a 6f 85 da f3 bd   ?...sM.2.?.o.??.
0080 : c7 d5 a5 e4 e7 13 9d 9b a4 a3 27                  ??..?.....'

C : Sending 6 bytes (Cipher Change)
```

```
0000 : 14 03 01 00 01 01                                  ......

C : Plaintext 16 bytes (Finished)
0000 : 14 00 00 0c c4 be 77 0b e5 a1 c1 7c 17 e8 67 04   ......w..??|.?g.

C : Sending 41 bytes (Encrypted Finished)
0000 : 16 03 01 00 24 ee 6c e2 94 6e 17 d0 7f 86 dd a0   ....$?l?.n....??
0010 : 1b 09 18 4c 6b ed be 1e 22 38 a6 08 56 56 18 66   ...Lk?.."8?.VV.f
0020 : 31 bd 78 8d 7e c5 27 77 f0                        1.x.~.'w.

S : Received 7 bytes (Handshake Failure Alert, 20)
0000 : 15 03 01 00 02 02 14                              .......
```


A.6.2. Wrong Premaster - Connection Success

This example uses the same handshake parameters as Appendix A.6.1, but (incorrectly) uses the negotiated version in the RSA Client Key Exchange Premaster Secret, not the Client Hello version.

```
C : Sending 82 bytes (Client Hello requesting TLS 1.1,
    in a TLS 1.0 Record)
0000 : 16 03 01 00 4d 01 00 00 49 03 02 44 90 ba 62 c9   ....M...I..D.?b?
0010 : 90 f9 f6 58 77 e4 47 4d 54 68 d0 34 2d 58 01 58   .?.Xw.GMTh.4-X.X
0020 : 58 75 9d 2d a9 7f 7f b0 31 79 2c 00 00 22 00 39   Xu.-...?1y,.."?9
0030 : 00 38 00 37 00 36 00 35 00 33 00 32 00 31 00 30   .8.7.6.5.3.2.1.0
0040 : 00 2f 00 05 00 04 00 13 00 0d 00 16 00 10 00 0a   ./..............
0050 : 01 00                                             ..

S : Received 948 bytes (Server Hello TLS 1.0)
0000 : 16 03 01 00 4a 02 00 00 46 03 01 44 90 b9 ca c7   ....J...F..D..??
0010 : e2 39 41 9b 19 83 f1 da 9f 28 19 44 4b 1e aa 60   ?9A...??.(.DK.?`
0020 : 16 8b d4 e5 a3 76 22 44 3f 99 12 20 2a c7 7a ed   ..?..v"D... *?z?
0030 : b1 22 97 0f 50 4d ee b1 a7 78 10 8c 59 aa bf 16   ."..PM?..x..Y??.
0040 : a5 19 75 bc f8 b1 6a eb 68 f6 0f 3d 00 05 00      ..u...j?h..=...

    (Certificate)
0040 :                                          16             .
0050 : 03 01 03 57 0b 00 03 53 00 03 50 00 03 4d 30 82   ...W...S..P..M0.
0060 : 03 49 30 82 02 b2 a0 03 02 01 02 02 03 3f 84 41   .I0...?........A
0070 : 30 0d 06 09 2a 86 48 86 f7 0d 01 01 04 05 00 30   0...*.H.?......0
0080 : 81 ce 31 0b 30 09 06 03 55 04 06 13 02 5a 41 31   .?1.0...U....ZA1
```

```
0090 : 15 30 13 06 03 55 04 08 13 0c 57 65 73 74 65 72   .0...U....Wester
00a0 : 6e 20 43 61 70 65 31 12 30 10 06 03 55 04 07 13   n Cape1.0...U...
00b0 : 09 43 61 70 65 20 54 6f 77 6e 31 1d 30 1b 06 03   .Cape Town1.0...
00c0 : 55 04 0a 13 14 54 68 61 77 74 65 20 43 6f 6e 73   U....Thawte Cons
00d0 : 75 6c 74 69 6e 67 20 63 63 31 28 30 26 06 03 55   ulting cc1(0&..U
00e0 : 04 0b 13 1f 43 65 72 74 69 66 69 63 61 74 69 6f   ....Certificatio
00f0 : 6e 20 53 65 72 76 69 63 65 73 20 44 69 76 69 73   n Services Divis
0100 : 69 6f 6e 31 21 30 1f 06 03 55 04 03 13 18 54 68   ion1!0...U....Th
0110 : 61 77 74 65 20 50 72 65 6d 69 75 6d 20 53 65 72   awte Premium Ser
0120 : 76 65 72 20 43 41 31 28 30 26 06 09 2a 86 48 86   ver CA1(0&..*.H.
0130 : f7 0d 01 09 01 16 19 70 72 65 6d 69 75 6d 2d 73   ?......premium-s
0140 : 65 72 76 65 72 40 74 68 61 77 74 65 2e 63 6f 6d   erver@thawte.com
0150 : 30 1e 17 0d 30 35 30 36 32 31 31 31 30 37 33 39   0...050621110739
0160 : 5a 17 0d 30 36 30 36 32 31 31 31 30 37 33 39 5a   Z..060621110739Z
0170 : 30 5b 31 0b 30 09 06 03 55 04 06 13 02 4e 4f 31   0[1.0...U....NO1
0180 : 0d 30 0b 06 03 55 04 08 13 04 4f 73 6c 6f 31 0d   .0...U....Oslo1.
0190 : 30 0b 06 03 55 04 07 13 04 4f 73 6c 6f 31 14 30   0...U....Oslo1.0
01a0 : 12 06 03 55 04 0a 13 0b 47 4f 54 4f 47 41 54 45   ...U....GOTOGATE
01b0 : 20 41 53 31 18 30 16 06 03 55 04 03 13 0f 77 77    AS1.0...U....ww
01c0 : 77 2e 67 6f 74 6f 67 61 74 65 2e 6e 6f 30 81 9f   w.gotogate.no0..
```



```
01d0 : 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03   0...*.H.?.......
01e0 : 81 8d 00 30 81 89 02 81 81 00 ca e1 b4 e6 2a cb   ...0......???.*?
01f0 : 27 c0 d3 17 d0 f8 8b 91 62 f9 97 84 86 b5 9e 0b   '??.....b?......
0200 : 1d df 97 b1 ce 7e 12 25 59 f2 80 d2 bf 8e 7b 56   .....?~.%Y?.??.{V
0210 : d0 cb 3c 1a ba c9 c6 0f 50 5b 17 b6 fd 66 ed c3   .?<.??..P[..?f??
0220 : 32 29 9b cd bb fd a4 9a 5a c1 67 48 2e 61 fa a6   2).?.?..Z?gH.a??
0230 : 48 1d ef 63 3c 97 38 6e a5 48 4c d8 e1 fe ec ec   H.?c<.8n.HL.?.??
0240 : ce 49 5a 86 54 43 ff 40 f2 8e 4c 26 35 d8 a3 19   ?IZ.TC?@?.L&5...
0250 : c6 e1 b9 6e ac 45 17 1d 37 32 85 18 d0 e3 41 d8   .?.n.E..72...?A.
0260 : c3 21 7b 67 e7 4f 37 64 f8 a9 02 03 01 00 01 a3   ?!{g?O7d........
0270 : 81 a6 30 81 a3 30 1d 06 03 55 1d 25 04 16 30 14   .?0..0...U.%..0.
0280 : 06 08 2b 06 01 05 05 07 03 01 06 08 2b 06 01 05   ..+.........+...
0290 : 05 07 03 02 30 40 06 03 55 1d 1f 04 39 30 37 30   ....0@..U...9070
02a0 : 35 a0 33 a0 31 86 2f 68 74 74 70 3a 2f 2f 63 72   5?3?1./http://cr
02b0 : 6c 2e 74 68 61 77 74 65 2e 63 6f 6d 2f 54 68 61   l.thawte.com/Tha
02c0 : 77 74 65 50 72 65 6d 69 75 6d 53 65 72 76 65 72   wtePremiumServer
02d0 : 43 41 2e 63 72 6c 30 32 06 08 2b 06 01 05 05 07   CA.crl02..+.....
02e0 : 01 01 04 26 30 24 30 22 06 08 2b 06 01 05 05 07   ...&0$0"..+.....
02f0 : 30 01 86 16 68 74 74 70 3a 2f 2f 6f 63 73 70 2e   0...http://ocsp.
0300 : 74 68 61 77 74 65 2e 63 6f 6d 30 0c 06 03 55 1d   thawte.com0...U.
0310 : 13 01 01 ff 04 02 30 00 30 0d 06 09 2a 86 48 86   ...?..0.0...*.H.
```

```
0320 : f7 0d 01 01 04 05 00 03 81 81 00 60 28 92 bc 07   ?..........`(...
0330 : 1f 96 76 d8 26 bd 10 59 8a 02 17 f3 a3 60 bc fc   ..v.&..Y...?.`..
0340 : 2a 4e b1 41 17 85 b3 b2 b0 4d db 43 d8 a4 f2 a9   *N.A....?M?C..?.
0350 : 7d 41 80 6d e7 fd ac 13 65 59 8c f3 81 6b 7c 0a   }A.m??..eY.?.k|.
0360 : b7 17 0d 00 4e 71 f4 84 f5 d2 30 b1 98 34 4b 2c   ?...Nq?.??0..4K,
0370 : b0 d0 0b 6d 85 e9 4d 6d 10 56 90 bd 36 b5 f3 5e   ?..m.?Mm.V..6.?^
0380 : ed 21 72 93 21 fc 90 d9 78 92 08 8b 6b b2 e9 0c   ?!r.!..?x...k.?.
0390 : 5a 19 54 b9 1a c9 ed c2 59 72 44 d3 13 57 08 15   Z.T..???YrD?.W..
03a0 : 1a 32 dd d9 53 23 85 76 d1 1c 0d 16 03 01 00 04   .2??S#.v?.......

     (Hello Done)
03b0 : 0e 00 00 00                                      ....

C : Plain Premaster Secret (Wrong version v3.1, negotiated version)
0000 : 03 01 9d 41 00 f3 76 57 07 9b 68 f9 d2 2d 5e 49   ...A.?vW..h??-^I
0010 : 9f 09 20 02 f6 b2 bf a2 c5 cb c7 6c 0f 2f 0c e2   .. ...?..??l./.?
0020 : 95 92 27 2d a3 0b 9f 33 cc 17 5b 28 72 1b 12 42   ..'-...3?.[(r..B

C : Sending 139 bytes (Client Key Exchange)
0000 : 16 03 01 00 86 10 00 00 82 00 80 1c b1 e5 ca 77   ...............?w
0010 : 7f 30 81 80 70 1d 5f 39 26 5b d7 c4 5e db 46 73   .0..p._9&[?.^?Fs
0020 : be 48 1a eb 92 fa 95 cd dc 23 f4 2a fe 7c 25 7f   .H.?.?.?.#?*.|%.
0030 : 0d d4 22 1f 48 f6 77 c2 a2 e4 53 49 ea f8 bf c4   .?".H.w?..SI?.?.
0040 : cf 34 12 98 46 93 d9 e2 b3 bc 10 f8 f3 c0 16 6e   ?4..F.??....??.n
0050 : 18 40 f7 8d c0 27 11 1f 04 30 f5 9b cd 42 c8 e5   .@?.?'...0?.?B?.
0060 : 1a e1 de 58 90 e6 b2 90 d4 89 19 ec bc 6b 29 cb   .?.X....?..?.k)?
0070 : 4d 62 01 38 26 ae 15 1c f5 21 13 b6 99 33 86 01   Mb.8&...?!...3..
```



```
0080 : 66 1b a3 10 e2 1d 72 c2 10 7e 64                  f...?.r?.~d

C : Sending 6 bytes (Cipher Change)
0000 : 14 03 01 00 01 01                                 ......

C : Plain Finished
0000 : 14 00 00 0c e8 e7 48 a2 d4 6e 0f a0 70 bf 3e 05   ....??H.?n.?p?>.

C : Sending 41 bytes (Encrypted Finished)
0000 : 16 03 01 00 24 6f 2f 39 d4 7d 78 84 89 15 c8 92   ....$o/9?}x...?.
0010 : bc de af 63 c9 53 2e c6 d6 27 01 5d 3c 96 00 1a   ..?c?S...'.]<...
0020 : ca e0 66 11 43 55 4e 2a ab                        ??f.CUN*.

S : Received 47 bytes (Cipher Change, Encrypted Finished)
```

```
0000 : 14 03 01 00 01 01 16 03 01 00 24 e7 6f 04 fc c8   ..........$?o..?
0010 : 9b c3 62 ae 27 bc cc 1a a0 01 f0 16 f3 7a cf cd   .?b.'.?.?...?z??
0020 : f7 8c db 16 60 4a a3 7b 3e c2 66 ad ef c6 f8      ?.?.`J.{>?f??..

S : Plaintext 16 bytes (Plaintext Finished)
0000 : 14 00 00 0c be 82 73 55 1b 12 ce 7c 25 02 4c af   ......sU..?|%.L?

<Connection established>
```

A.7. Refusing to accept compression methods

Contributed by: Pasi Eronen

This example shows a TLS 1.0 client that requests LZS compression [RFC3943] (code 64) and the Null method. The server responds with a Handshake Failure Alert message.

```
C: Sending 53 bytes: (TLS 1.0 Client hello, in TLS 1.0 Record, requesting
   LZS (code 64) and Null compression methods)
0000 : 16 03 01 00 30 01 00 00 2c 03 01 6b c6 db 2a 4c
0000 : 64 3e 05 df 2f 15 20 ab 7e e6 7a d1 eb 9c 20 59
0000 : 2a ea 83 d4 3f 37 ea 98 3b 3c 87 00 00 04 00 2f
0000 : 00 0a 02 40 00

S: Received 7 bytes: (Alert message: Handshake failure)
0000 : 15 03 01 00 02 02 28
```

A.8. Copying the Client Hello Version field

Date: July 22, 2006

Server: (As identifed in the HTTP Server Header) OfficeLine 3.5 Webserver (2.16)

Site: https://ebssl.unibanka.sk

Highest supported version: SSL v3.0

This example shows a specially modified client use a TLS 1.0 Client Hello, in a TLS 1.0 Record, to request a connection using the hypothetical SSL v4.0 protocol. Even though the server only supports SSL v3.0 it incorrectly responds with {4.0} as the selected version. Similar incorrect selections have been observed for TLS 1.0 and TLS 1.1 versions numbers, which inevitably results in Handshake Failure errors.

```
C: Sending 82 bytes (TLS 1.0 Record and TLS 1.0 Client Hello, specifying
  non-existen version {4,0} as the highest supported.
0000 : 16 03 02 00 4d 01 00 00 49 04 00 44 c1 6e 9e f8   ....M...I..D.n..
0010 : 26 c8 01 44 01 be 98 0a 04 03 92 2e 35 46 26 0f   &..D........5F&.
0020 : 4e aa c9 0d 14 da 51 f3 b0 56 6f 00 00 22 00 39   N.....Q..Vo..".9
0030 : 00 38 00 37 00 36 00 35 00 33 00 32 00 31 00 30   .8.7.6.5.3.2.1.0
0040 : 00 2f 00 05 00 04 00 13 00 0d 00 16 00 10 00 0a   ./..............
0050 : 01 00                                             ..

S : Recieved 63 bytes (Server Hello/Record specifying 4.0 as the version,
    although the server only supports SSL v3.0 as its highest version)
0000 : 16 04 00 00 3a 02 00 00 36 04 00 44 c1 8b cd 5d   ....:...6..D...]
0010 : 53 d3 c0 c8 ef ce cb bd da 0b e5 50 ef fa 21 69   S..........P..!i
0020 : 63 d5 9e 54 7b ad 1f 98 34 5c 56 10 97 d3 90 04   c..T{..4\V.....
0030 : cd 8b c1 44 97 d3 90 04 8d ac 21 00 00 04 00      ...D......!....
```

Author's Address

Yngve N. Pettersen
Opera Software ASA
Waldemar Thranes gate 98
N-0175 OSLO,
Norway

Email: yngve@opera.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).