0. Abstract

Network Working Group T. Dierks Request for Comments: 5246 Independent Obsoletes: 3268, 4346, 4366 E. Rescorla Updates: 4492 RTFM, Inc. Category: Standards Track August 2008

```
            The Transport Layer Security (TLS) Protocol
                           Version 1.2
```

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the “Internet Official Protocol Standards” (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This document specifies Version 1.2 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

Table of Contents

1. Introduction ....4 1.1. Requirements Terminology ....5 1.2. Major Differences from TLS 1.1 5

2. Goals 6

3. Goals of This Document 7

4. Presentation Language ....7 4.1. Basic Block Size ....7 4.2. Miscellaneous ....8 4.3. Vectors ....8 4.4. Numbers ....9 4.5. Enumerateds ....9 4.6. Constructed Types ....10 4.6.1. Variants ....10 4.7. Cryptographic Attributes ....12 4.8. Constants 14

5. HMAC and the Pseudorandom Function 14

6. The TLS Record Protocol ....15 6.1. Connection States ....16 6.2. Record Layer ....19 6.2.1. Fragmentation 19

6.2.2. Record Compression and Decompression 20
6.2.3. Record Payload Protection 21
6.2.3.1. Null or Standard Stream Cipher 22
6.2.3.2. CBC Block Cipher 22
6.2.3.3. AEAD Ciphers 24

6.3. Key Calculation 25

7. The TLS Handshaking Protocols 26
7.1. Change Cipher Spec Protocol 27
7.2. Alert Protocol 28
7.2.1. Closure Alerts ....29 7.2.2.
Error Alerts ....30 7.3. Handshake Protocol Overview ....33 7.4.
Handshake Protocol 37
7.4.1. Hello Messages 38
7.4.1.1. Hello Request ....38 7.4.1.2.
Client Hello ....39 7.4.1.3. Server Hello
.............................42 7.4.1.4. Hello Extensions 44
7.4.1.4.1. Signature Algorithms ....45 7.4.2. Server Certificate ....47 7.4.3. Server Key
Exchange Message ....50 7.4.4. Certificate
Request ....53 7.4.5. Server Hello
Done ....55 7.4.6. Client Certificate
................................55 7.4.7. Client Key Exchange Message
........................57 7.4.7.1. RSA-Encrypted Premaster Secret
Message ....58 7.4.7.2. Client Diffie-Hellman Public Value ....61 7.4.8.
Certificate Verify ....62 7.4.9. Finished
....63

8. Cryptographic Computations ....64 8.1.
Computing the Master Secret ....64 8.1.1. RSA
....65 8.1.2. Diffie-Hellman
....................................65

9. Mandatory Cipher Suites 65

10. Application Data Protocol 65

11. Security Considerations 65

12. IANA Considerations 65
Appendix A. Protocol Data Structures and Constant Values 68
A.1. Record Layer 68
A.2. Change Cipher Specs Message 69
A.3. Alert Messages 69
A.4. Handshake Protocol 70
A.4.1. Hello Messages ....71 A.4.2.
Server Authentication and Key Exchange Messages ....72 A.4.3. Client

Authentication and Key Exchange Messages . . . .74 A.4.4. Handshake Finalization Message . . . . 74 A.5. The Cipher Suite . . . . 75 A.6. The Security Parameters 77

`A.7. Changes to RFC 4492` 78

Appendix B. Glossary 78
Appendix C. Cipher Suite Definitions 83
Appendix D. Implementation Notes 85
D.1. Random Number Generation and Seeding 85
D.2. Certificates and Authentication . . . . 85 D.3. Cipher Suites . . . . 85 D.4. Implementation Pitfalls . . . . .85 Appendix E. Backward Compatibility . . . . .87 E.1. Compatibility with TLS 1.0/1.1 and SSL 3.0 . . . . .87 E.2. Compatibility with SSL 2.0 . . . . .88 E.3. Avoiding Man-in-the-Middle Version Rollback . . . . 90 Appendix F. Security Analysis . . . . .91 F.1. Handshake Protocol . . . . .91 F.1.1. Authentication and Key Exchange .91 F.1.1.1. Anonymous Key Exchange .91 F.1.1.2. RSA Key Exchange and Authentication . . . . . . .92 F.1.1.3. Diffie-Hellman Key Exchange with Authentication . . . . .92 F.1.2. Version Rollback Attacks . . . . 93 F.1.3. Detecting Attacks Against the Handshake Protocol . . . 94 F.1.4. Resuming Sessions 94
F.2. Protecting Application Data . . . . .94 F.3. Explicit IVs . . . . .95 F.4. Security of Composite Cipher Modes . . . . 95 F.5. Denial of Service . . . . .96 F.6. Final Notes . . . . .96 Normative References . . . . .97 Informative References . . . . .98 Working Group Information . . . . .101 Contributors 101