SSL and TLS: Theory and Practice

Chapter 7 – Concluding Remarks

Rolf Oppliger

May 28, 2023

Terms of Use

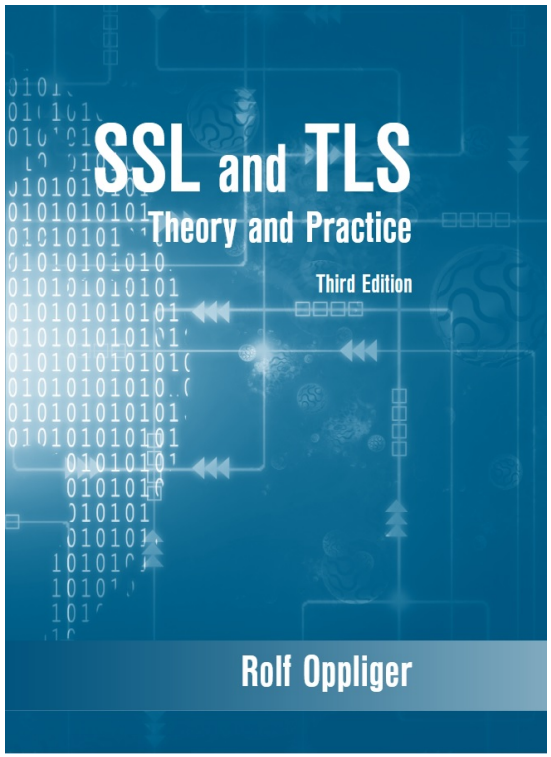
- This work is published with a CC BY-ND 4.0 license ()
  - CC = Creative Commons ()
  - BY = Attribution ()
  - ND = No Derivatives ()

whoami

`rolf-oppliger.ch`
`rolf-oppliger.com`

- eSECURITY Technologies Rolf Oppliger (founder and owner)
- Swiss National Cyber Security Centre NCSC (scientific employee)
- University of Zurich (adjunct professor)
- Artech House (author and series editor for information security and privacy)

Reference Book



ISBN 978-1-68569-015-1

`https://www.esecurity.ch/Books/ssltls3e.html`

Challenge Me

Outline

7. Concluding Remarks

1. Statistics are available from many online resources (e.g., Qualys SSL Labs' SSL Pulse) and trade press articles

   Most statistics bear witness to the facts

   - that the use of the SSL/TLS protocols is steadily increasing
   - that SSL/TLS is by far the predominant security technology on the internet

7. Concluding Remarks

2. An immediate consequence of SSL/TLS's triumphant advance is that its security is subject to a lot of public scrutiny (i.e., many attacks have been found and mitigated)

   Some vulnerabilities and attacks are devastating and indeed frightening

   Still the most important example is Heartbleed

7. Concluding Remarks

3. There are several documents that elaborate on how to configure a system that implements the SSL/TLS and DTLS protocols in a secure way (e.g., RFC 9325)

   Cipher suites recommended for TLS 1.2

   - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
   - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

   For TLS 1.3, the recommended cipher suites are provided in the specification

7. Concluding Remarks

4. TLS 1.3 is a true security milestone in the evolution of the SSL/TLS protocols

   TLS 1.3 is the first protocol version that is severely restricted to using only strong cryptography (e.g., AEAD ciphers and key exchange methods that always provide forward secrecy)

   The story continues . . .

Questions and Answers

Thank you for your attention