Vorlesung Netzwerksicherheit – Sommersemester 2021

3. Übungszettel

Abgabe: Bis Dienstag, 11. Mai 2021 – 16:00 Uhr
Besprechung: Dienstag, 11. Mai 2021

Abgabe in Gruppen von 2-3 Personen (Name + Matrikelnummer angeben)

Abgabe per Mail an: wueb+Uebung03@cs.uni-bonn.de

Aufgabe 1 (5 Punkte)

Geben sie die Funktionsweise des in der Vorlesung gezeigten TLS Handshake Protocols in eigenen Worten wieder. Erläutern sie dabei ausführlich welche Informationen in den einzelnen Schritten geteilt oder abgefragt werden und welchem Zweck die einzelnen Schritte dienen.

Aufgabe 2 (5 Punkte)

Bezogen auf das ISO/OSI-Schichtenmodell lässt sich TLS in den Schichten Session und Presentation verorten. Begründen Sie diese Tatsache für beide Schichten ausführlich und stellen Sie den Zusammenhang von der Transport bis zur Anwendungsschicht dar.

Aufgabe 3 (3 Punkte)

Auf welche Schicht des TCP/IP-Modell verorten Sie TLS? Welche Folgen hat das für den Zusammenhang zwischen Transport und Anwendungsschicht? Begründen Sie Ihre Annahme ausführlich.

Aufgabe 4 (5 + 2 Punkte)

In der Vorlesung wurde diskutiert, dass Webbrowser und Webserver nicht alle TLS-Cipher-Suites unterstützen.

a) Finden Sie heraus, welche Cipher-Suite ihre TLS-Bibliothek (OpenSSL, Gnutls, etc.) zur Verfügung stellt und vergleichen Sie diese mit der Liste in Ihrem Browser. Dokumentieren Sie die durchgeführten Schritte und geben Zwischenergebnisse mit an.
b) Mit welchen Cipher-Suites können Sie eine Verbindung zum Big Blue Button der Vorlesung aufbauen? Dokumentieren Sie die durchgeführten Schritte und geben Zwischenergebnisse mit an.