Christian Schindelhauer

Freiburg, den 23. Mai 2012
Besprechung 5. Juni 2012

Übungen zur Vorlesung

Systeme II / Netzwerke I

Sommer 2012

Blatt 5

AUFGABE 1:
Sie bauen eine SSL Verbindung mit dem Server *https://scipio.informatik.uni-freiburg.de/* auf. Ihr Browser gibt Ihnen dabei Rückmeldung über das vom Server verwendete Zertifikat.

a) Wie entscheidet Ihr Browser, ob das Zertifikat (un-)gültig ist?

b) Vergleichen Sie das Zertifikat mit dem von *google.de* und geben Sie den Zertifizierungspfad an.

c) Sie bauen nun die SSL Verbindung zum Uni-Server auf. Ist Ihre Verbindung verschlüsselt?

d) Bei Aufbau einer SSL Verbindung wird ein sogenannter *pre-master-secret* erzeugt. Wie wird dieser erzeugt und welches Verschlüsselungsverfahren wird dabei verwendet?

e) Wie wird nach der Erzeugung des *Master Secret* kommuniziert?

f) Die Verbindung kann nach einem erfolgreichen Verbindungsaufbau gefährdet sein. Von welchem maßgeblichen Aspekt hängt die Sicherheit ab?

AUFGABE 2:
Wireshark

a) Installieren Sie Wireshark und machen Sie sich mit der Oberfläche vertraut.

b) Senden oder empfangen Sie Mails und beobachten Sie dabei den aufgezeichneten Traffic. Können Sie aus den aufgezeichneten Paketen Username, Passwort oder Nachrichtentext entnehmen?

c) Wählen Sie eines der angezeigten Pakete aus und schlüsseln Sie dieses in seine Schichten auf.