Vorlesung Netzwerksicherheit – Sommersemester 2022

12. Übungszettel

Abgabe bis Dienstag, 12. Juli 2022 – 16:00 Uhr
Besprechung: Dienstag, 12. Juli 2022

Abgabe in festen Gruppen (Namen + Matrikelnummern angeben)

Abgabe via Artemis: https://alpro.besec.uni-bonn.de

Aufgabe 1 (5 Punkte)

Beschreiben Sie den Unterschied der Begriffe Authentisierung und Authentifizierung. Verwenden Sie dabei *nicht* die in der Vorlesung verwendete Analogie eines Personalausweises.

Aufgabe 2 (6 Punkte)

Beantworten Sie die folgenden Fragen zu Shared-Secrets:

a) Was ist ein Shared-Secret und wofür kann es verwendet werden?
b) Warum eignen sich Shared-Secrets zur Authentifikation im Internet?
c) Warum sollten Shared-Secrets beim Diensteanbieter nicht im Klartext abgespeichert werden und welche Verfahren kennen Sie, wo dies trotzdem notwendig ist?

Aufgabe 3 (6 Punkte)

a) Beschreiben Sie in eigenen Worten die Funktionsweise von FIDO2, fokussieren Sie sich dabei insbesondere auf die notwendigen Schritte aus Sicht von Client und Server.
b) Geben Sie an, welche Schritte bei FIDO2 zur Authentisierung und welche zur Authentifizierung zählen.

Aufgabe 4 (2 + 1 Punkte)

a) Testen Sie den Login unter https://webauthn.io und dokumentieren Sie Ihren Versuch mit zwei Screenshots.
b) Eignet sich FIDO2 für die Zugangskontrolle von Wireguard? Würden Sie diese Anwendung empfehlen oder davon abraten?