

12. Übungszettel

Abgabe: Bis Dienstag, 20. Juli 2021 – 16:00 Uhr

Besprechung: Dienstag, 20. Juli 2021

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

Abgabe via Artemis

Aufgabe 1 (6 Punkte)

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

Aufgabe 2 (7,5 Punkte)

- 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 (2 + 1,5 Punkte)

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

Aufgabe 4 (2 + 1 Punkte)

- a) Testen Sie den Login unter 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?