Vorlesung Netzwerksicherheit – Sommersemester 2021

**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)**

1. Was ist ein Shared-Secret und wofür kann es verwendet werden?
2. Warum eignen sich Shared-Secrets zur Authentifikation im Internet?
3. 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)**

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

**Aufgabe 4 (2 + 1 Punkte)**

1. Testen Sie den Login unter webauthn.io und dokumentieren Sie Ihren Versuch mit zwei Screenshots.
2. Eignet sich FIDO2 für die Zugangskontrolle von Wireguard? Würden Sie diese Anwendung empfehlen oder davon abraten?