IT-Security Tutorübung 08

Dorian Zedler

11. Dezember 2023

Technische Universität München

Inhalt der Tutorübung

Aufgabe 1

Aufgabe 2

Aufgabe 3

Aufgabe 4

Inhalt der Tutorübung

- Authentifizierung
- Biometrie
- OTP
- Challenge-Response

Aufgabe 1

Aufgabe 1a - Pseudonymisierung vs. Ananonysierung

a) Was ist der Unterschied zwischen Pseudonymisierung und Anonymisierung?
   - **Pseudonymisierung**: Klarname kann durch Hinzuziehen zusätzlicher Daten (z.B. Tabelle) wiederhergestellt werden. Beispiele: Matrikelnummer, TUM-Kennung
   - **Anonymisierung**: Klarname kann nicht wiederhergestellt werden.

Aufgabe 1b - Basisfaktoren für Authentifizierung

b) Nennen Sie die drei Basisfaktoren, auf denen Authentifizierung beruhen kann und nennen Sie jeweils ein Beispiel für ein Authentifizierungsmerkmal für diesen Faktor.

- **Wissen**: Passwort, PIN, Schlüssel
- **Besitz**: Smartcard, Token, SIM-Karte
- **Biometrie**: Fingerabdruck, Gesicht, Iris

Aufgabe 1c - Multi-Faktor-Authentifizierung

c) Was ist Multi-Faktor Authentifizierung und welchen Vorteil bringt diese mit sich?

- Kombination mehrerer Authentifizierungsfaktoren
  →**Alle** Faktoren müssen korrekt präsentiert werden
- Vorteil: erhöhte Sicherheit
  →Ein Angreifer muss alle Faktoren kompromittieren
- Beispiel: Passwort und YubiKey

Aufgabe 1d - Biometrische Merkmale

d) Erläutern Sie die Anforderungen an biometrische Merkmale

- **Universalität:** Jede Person besitzt das Merkmal.
- **Eindeutigkeit:** Das Merkmal identifiziert jede Person (relativ) eindeutig.
- **Beständigkeit:** Das Merkmal ist unveränderlich und degradiert nicht über die Zeit.
- **Quantitative Erfassbarkeit:** Das Merkmal lässt sich mittels eines Sensors erfassen und verarbeiten.
- **Performance:** Das Merkmal muss genau genug und schnell genug erfasst werden können.
- **Akzeptanz:** Für einen Benutzer muss es akzeptabel sein, dass das Merkmal erfasst und für die Authentifikation verwendent wrid.
- **Fälschungssicherheit:** Es darf nicht einfach möglich sein das Merkmal einer Person zu fälschen.

Aufgabe 12 - Enrollment

2) Erläutern Sie den Begriff *Enrollment* bei biometrischer Authentisierung!
   - Registrierung eines neuen Nutzers
   - Erfassung uns Speicherung der biometrischen Merkmale

Aufgabe 2

Aufgabe 2a - Kennzahlen für biometrische Authentifizierung

a) Erklären Sie im Kontext von Authentifikation mittels Biometrie die Begriffe *False Negative*, *False Positive*, *False Acceptance Rate* (FAR) und *False Rejection Rate* (FRR)!

- **False Negative:** Ein berechtigter Nutzer wird fälschlicherweise abgewiesen.
- **False Positive:** Ein unberechtigter Nutzer wird fälschlicherweise authentifiziert.
- **False Acceptance Rate:** Wahrscheinlichkeit für die fälschliche Akzeptanz einer Person (False Positive).
- **False Rejection Rate:** Wahrscheinlichkeit für die fälschliche Rückweisung einer berechtigten Person (False Negative).

Aufgabe 2b - Kennzahlen für biometrische Authentifizierung

- Für eine Hochsicherheitsanwendung soll ein biometrisches Authentifizierungsverfahren eingesetzt werden.
- Es gibt drei Möglichkeiten mit folgenden Kenndaten:

Name	Preis	FAR	FRR	DPI
Fluxfinger Checker	10	0.1 %	0.1 %	250
Pro Finger	25	0.01 %	0.1 %	200
Excellent Finger	50	0.2 %	0.01 %	250

b) Welches Gerät eignet sich für das vorgestellte Szenario am besten? Begründen Sie Ihre Entscheidung!

- Das Gerät **Pro Finger** ist am besten für die Einlasskontrolle geeignet, da dieses Gerät die niedrigste **False Acceptance Rate** besitzt.

Aufgabe 3

Aufgabe 3a - OTP

a) Definieren Sie den Begriff One-Time-Passwort (OTP)! Welche Arten von OTPs kennen Sie und wo finden Sie Anwendung?

- **Definition:** OTPs sind Passwörter, die nur einmal verwendet werden können. Meist werden sie periodisch automatisiert generiert (TOTP).
- **Arten:**
  - Softwarebasiert oder Hardwarebasiert
  - Zeitbasiert oder Challenge-Response
  - Beispiele:

    Google Authenticator: Softwarebasiert, Zeitbasiert

    YubiKey: Hardwarebasiert, Challenge-Response
- **Anwendung:**
  - Zwei-Faktor-Authentifizierung
  - TAN Verfahren für Überweisungen
  - Passwort-Reset

Aufgabe 3b - OTP

b) Vergleichen Sie die Funktionsweise des *RSA SecurID-Token* und des *Google Authenticators*. Wie unterscheiden sie sich?

	RSA SecureID-Token	**Google Authenticator**
Hard/Soft	Hardwarebasiert	Softwarebasiert
Zeit/Challenge	Zeitbasiert	Zeitbasiert
Algorithmus	AES	HMAC-SHA1
Angreifbarkeit	Diebstahl	Malware / Schlüsselübertragung

- Beim Google Authenticator müssen die Schlüssel an die App übertragen werden (SMS, QR-Code, etc)
  $\rightarrow$Angriffsmöglichkeit (z.B. bösartiger QR-Code Scanner, kompromittierte TLS-Verbindung mit Authentifizierungsserver etc)
- Beim RSA-Token ist der Schlüssel in der Hardware kodiert und wird nie übertragen
  $\rightarrow$Angriff auf Softwarebasis unmöglich

Aufgabe 3c - OTP

c) Verhindern OTPs *Phishing*-Angriffe?

- **NEIN**
- Eine Phishing-Webseite kann die OTPs einfach an den Server weiterleiten und sich so authentifizieren.
- Grundlegendes Problem: Webseite authentifiziert sich nicht gegenüber dem Nutzer
- Lösung: **FIDO2** (nicht Teil der Vorlesung)

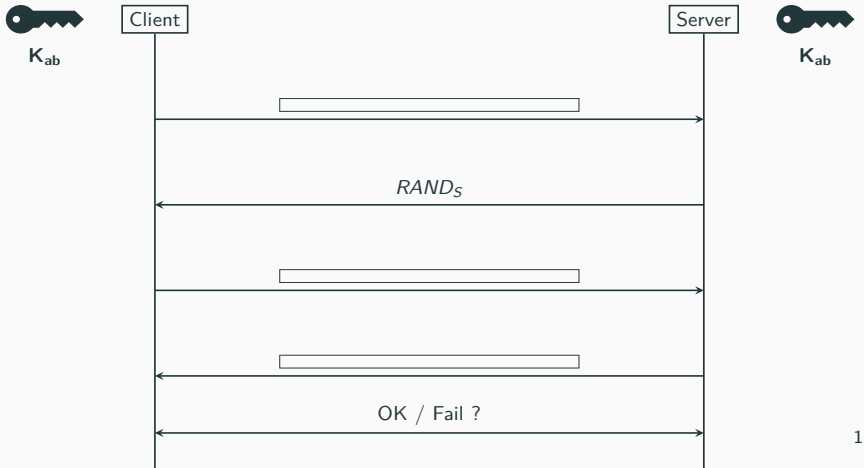
Aufgabe 4

Aufgabe 4 - Challenge-Response

- Server und Client wollen sich gegenseitig authentifizieren
- Im Vorfeld wurde ein gemeinsamer Schlüssel K_{AB} vereinbart
- Es stehen nur ein Zufallszahlengenerator und AES zur Verfügung

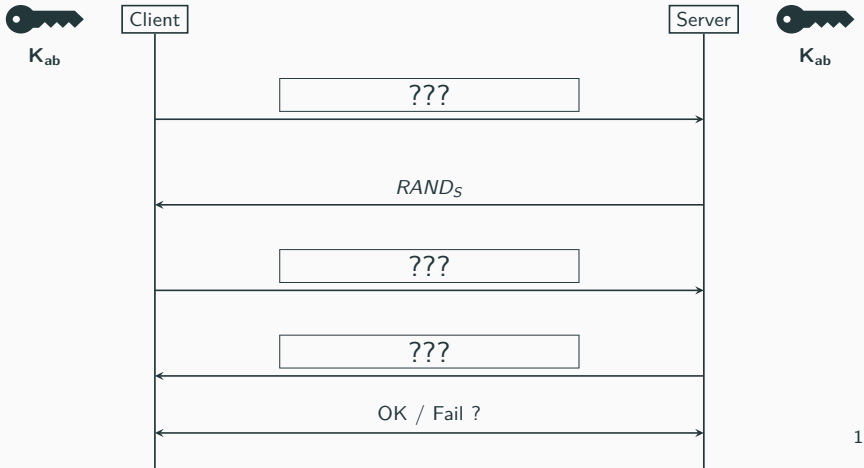
Aufgabe 4a - Challenge-Response

a) Vervollständigen Sie das oben skizzierte Protokoll zur *Challenge-Response-Authentifizierung*!



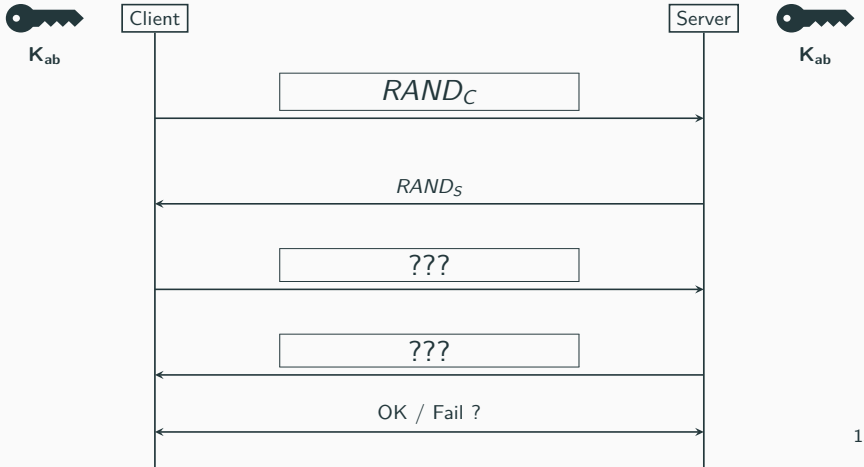
Aufgabe 4a - Challenge-Response

a) Vervollständigen Sie das oben skizzierte Protokoll zur *Challenge-Response-Authentifizierung*!



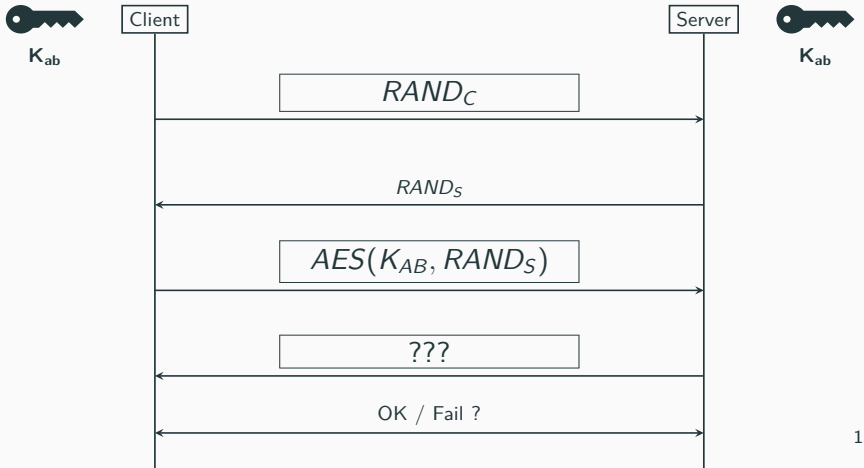
Aufgabe 4a - Challenge-Response

a) Vervollständigen Sie das oben skizzierte Protokoll zur *Challenge-Response-Authentifizierung*!



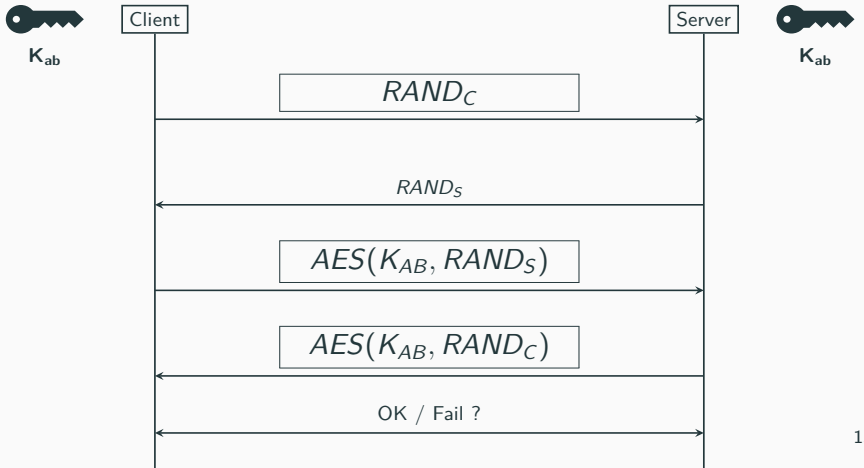
Aufgabe 4a - Challenge-Response

a) Vervollständigen Sie das oben skizzierte Protokoll zur *Challenge-Response-Authentifizierung*!



Aufgabe 4a - Challenge-Response

a) Vervollständigen Sie das oben skizzierte Protokoll zur *Challenge-Response-Authentifizierung*!



Aufgabe 4b - Challenge-Response

b) Welchen Vorteil bietet eine *Challenge-Response-Authentifizierung* gegenüber einer, die auf einem Passwort basiert?

- Beim passiven Abhören kann ein Angreifer das Passwort nicht aus der Aufzeichnung rekonstruieren.

Aufgabe 4c - Challenge-Response

c) Schützt Ihr Protokoll auch vor einem Replay Angriff?

- Solange $RAND_C$ und $RAND_S$ nicht wiederverwendet werden: **JA**
- In der Praxis meist so groß gewählt, dass Wiederverwendung unwahrscheinlich ist