

IT-Security Tutorübung 11

Dorian Zedler

14. Januar 2024

Technische Universität München

Aufgabe 1

Aufgabe 2

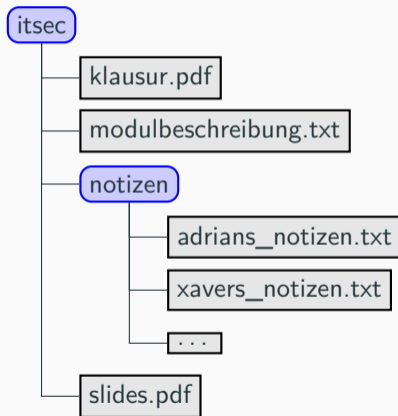
Aufgabe 3

- Unix File-Permissions
- Sicherer Web-Login
- Klausuraufgaben

Aufgabe 1

Aufgabe 1 - Unix File-Permissions

- Gegeben sei folgende Verzeichnisstruktur:



Aufgabe 1a - Unix File-Permissions

```
$ ls -l
-rw-r--rw- 1 claudia uebungsleitung 258K Dec 20 14:29 klausur.pdf
-rw-r--r-- 1 claudia studierende     5.9K Dec 21 09:34
↔ modulbeschreibung.txt
drwxrwx--T 1 fabian studierende     4.0K Dec 21 09:39 notizen
-rw-r----- 1 claudia studierende   1.6M Dec 21 09:34 slides.pdf
```

- a) Beschreiben Sie für jede Spalte der Ausgabe jeweils dessen Bedeutung.
- drwxrwx-: d steht für ein Verzeichnis, der Rest sind die Zugriffsrechte
 - 1: Hardlinks auf die Datei
 - fabian: Besitzer der Datei (als UID gespeichert)
 - studierende: Gruppe der Datei (als GID gespeichert)
 - 4.0K: Größe der Datei in Bytes
 - Dec 21 09:39: Zeitpunkt der letzten Änderung
 - notizen: Name der Datei / des Verzeichnisses

Aufgabe 1b - Unix File-Permissions

```
$ ls -l
-rw-r--rw- 1 claudia uebungsleitung 258K Dec 20 14:29 klausur.pdf
-rw-r--r-- 1 claudia studierende    5.9K Dec 21 09:34
↪ modulbeschreibung.txt
drwxrwx--T 1 fabian  studierende    4.0K Dec 21 09:39 notizen
-rw-r----- 1 claudia studierende    1.6M Dec 21 09:34 slides.pdf
```

- b) Fällt Ihnen ein Problem mit der Rechtevergabe wie oben dargestellt auf?
- Die datei `klausur.pdf` ist für alle lesbar und schreibbar
 - Studierende könnten die Klausur also schon vor dem Termin lesen und verändern
 - Die Übungsleitung kann die Klausur nicht verändern

Aufgabe 1c - Unix File-Permissions

- c) Was bedeuten die **read**, **write** und **execute** Zugriffsrechte bei Verzeichnissen?

Berechtigung	auflisten	verwalten ¹	verwenden ²

-w-			
r--	✓		
--x			✓
r-x	✓		✓
-wx		✓	✓
rxw	✓	✓	✓

¹Inhalte umbenennen, löschen, erstellen

²Metadaten der Inhalte einsehen und entsprechend der Berechtigungen lesen/bearbeiten/ausführen

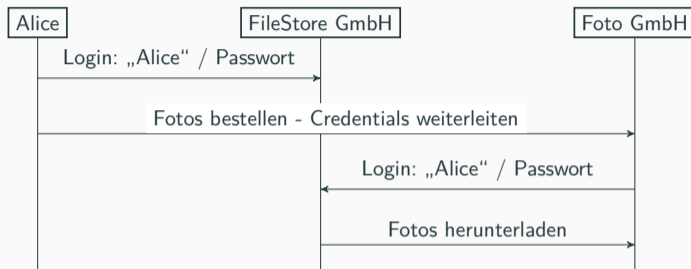
- d) Schlagen Sie das „sticky“ Bit nach und erklären Sie dessen Anwendung im oben gezeigten Beispiel.
- Beispiel: /tmp-Verzeichnis: jeder soll Dateien anlegen und löschen können, aber man soll keine Dateien anderer Nutzer löschen können!
 - Problem:
 - selbst, wenn man die Datei nicht lesen, schreiben und ausführen darf, kann man sie löschen und umbenennen, wenn man das Verzeichnis verwalten darf.
 - man muss das Verzeichnis aber verwalten dürfen, um Dateien anlegen und löschen zu können
 - Lösung: Das „sticky“ Bit beschränkt die *verwalten*-Berechtigung auf den Besitzer der Datei!

Aufgabe 1e - Unix File-Permissions - das setuid Bit

- e) Schlagen Sie nun ebenfalls die „setuid“ und „setgid“ Bits nach und erklären Sie deren Effekt und Anwendung auf *ausführbare* Dateien.
- Beispiel: Man möchte das eigene Passwort ändern.
 - Problem:
 - Passwort ist in der Datei `/etc/shadow` gespeichert
 - `/etc/shadow` darf nur von `root` geschrieben werden, damit man nicht die Passwörter aller Nutzer ändern kann
 - Lösung:
 - Wenn das „setuid“ bit gesetzt ist, wird das Programm mit den Rechten des Besitzers ausgeführt. Genauso analog für das „setgid“ Bit nur mit der Gruppe.
 - `passwd` ist ein Programm, das zuerst das aktuelle Passwort abfragt und dann das neue Passwort in `/etc/shadow` schreibt
 - die ausführbare Datei von `passwd` gehört `root` und hat das „setuid“ wird also mit den Rechten von `root` ausgeführt!

Aufgabe 2

Aufgabe 2a - Sicherer Web-Login



a) Beschreiben Sie, wodurch die drei Parteien authentifiziert sind!

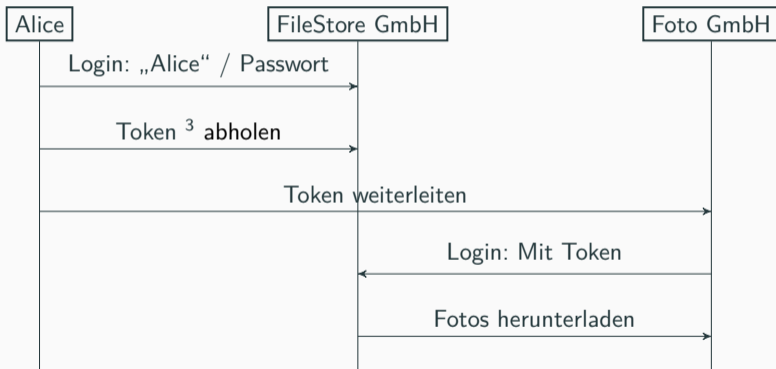
	Alice	FileStore GmbH	Foto GmbH
Alice	-	Passwort	Passwort
FileStore GmbH	TLS-Zertifikat	-	TLS-Zertifikat
Foto GmbH	TLS-Zertifikat	Alice's Passwort	-

b) Gibt es ein Sicherheitsproblem? Wenn ja, wo?

- **JA!**
- Die Foto GmbH kennt Alice's und kann auf alle ihre Dateien, nicht nur die bestellten Fotos, zugreifen!

Aufgabe 2c - Sicherer Web-Login - so gehts richtig!

- c) Mit welchem Protokoll der Vorlesung könnte das Problem gelöst werden?
Schlagen Sie einen neuen Protokollablauf vor und skizzieren Sie diesen!



³beschränkt auf read-only Zugriff auf die bestellten Fotos

Aufgabe 3

Aufgabe 3 - Klausuraufgabe Retake 22/23

Aufgabe 2 Protokollsicherheit (10 Punkte)

Für die folgende Aufgabe sei H eine kryptografisch sichere Hashfunktion und $F_k(m) = H(k \oplus 5c5c... || H(k \oplus 3636... || m))$. Des Weiteren seien E und D Ver- und Entschlüsselungsfunktion, die durch die Blockchiffre AES-128 im CBC-Modus mit PKCS7-Padding gebildet wird. $g \in \{2, \dots, p\}$ und p ist eine große Primzahl.

