Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2024/2025
Übungsblatt 9

Besprechung: Do, 09.01.2025 um 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Aufgabe 1: (T) Kryptographische Hashfunktionen

a. Welche Eigenschaften besitzen Hashfunktionen bzw. kryptographische Hashfunktionen?

b. Nennen Sie mindestens 2 Einsatzszenarien für (kryptographische) Hashfunktionen.

c. Was versteht man unter dem Begriff *Kollisionsresistenz*?

Aufgabe 2: (T) Salz und Pfeffer

Passworte der Nutzerverwaltung müssen i.d.R. in einer Art Datenbank der Anwendung gespeichert werden. Dies kann auf verschiedene Weisen geschehen, die jeweils andere Vor- und Nachteile mit sich bringen. Beschreiben und diskutieren Sie...

- Funktionsweise / Art der Speicherung
- Was sieht ein Angreifer im Leak?
- Welche „bösen Dinge“ können Angreifer damit anstellen?

der folgenden Methoden zur Speicherung von Benutzerpassworten:

a. Passwort im Klartext

b. Passwort nur als Hash

c. Passwort als salted Hash

d. Passwort als peppered salted Hash

Aufgabe 3: (T) Post Quantum Cryptography

a. Mosca's inequality – what's the problem?

b. Welche Bedrohung stellen Quantencomputer für Kryptosysteme dar? Sind symmetrische, asymmetrische und Hash-Funktionen gleichermaßen betroffen? Gilt das für alle Algorithmen/Kryptosysteme dieser Klassen?
Tipp: Shor, Grover, ...

c. Manche staatlichen Institutionen speichern Ciphertexte im großen Stil – zur späteren Entschlüsselung, sobald die nötige Rechenleistung dafür verfügbar sein wird. Ist das ein Problem?