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 2020/2021
Übungsblatt 9

Abgabetermin: 26.01.2021 um 12:00 Uhr

Aufgabe 18: (K) 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 19: (K) Authentisierung & One-Time Passwords

a. Zur Authentisierung von Benutzern werden bekanntlich verschiedene Verfahren eingesetzt, die sich unterschiedlichen Kategorien zuordnen lassen. Passwörter beispielsweise werden der Kategorie *Wissen* zugeordnet. Nennen Sie mindestens drei weitere geeignete Kategorien und geben Beispielverfahren aus der Praxis an. Benennen Sie auch Vor-/Nachteile der jeweiligen Kategorie oder des konkreten Verfahrens.

b. Betrachten Sie eine Web-Applikation, die Passwörter zur Nutzerauthentisierung einsetzt. Diese werden unverschlüsselt übertragen werden. Mallet snifft den kompletten Netztraffic mit und möchte die Zugangsdaten später wiederverwenden. Um welche Art von Angriff handelt es sich dabei am ehesten: Brute-Force-, Wörterbuch-, Social-Engineering- oder Replay-Angriff? Begründen Sie ihre Antwort und erläutern Sie die drei verbleibenden Antwortmöglichkeiten.

Aufgabe 20: (K) Biometrie

Biometrie wird heute immer häufiger zur Authentisierung verwendet. Die Nutzer erwarten in erster Linie Bequemlichkeit, während die Sicherheitsverantwortlichen auf eine höhere Sicherheit bei Finanztransaktionen und Bezahlvorgängen abzielen. Doch wo Chancen sind, sind meist auch Risiken.

a. Nennen Sie mindestens 5 Eigenschaften eines zur Authentisierung geeigneten biometrischen Merkmals.

b. Beschreiben Sie kurz in eigenen Worten die allgemeine Vorgehensweise bei Verwendung eines biometrischen Systems.

c. An welchen Stellen des in der vorherigen Aufgabe beschriebenen Ablaufs ist ein Angriff möglich? Geben Sie auch Beispiele für konkrete Gegenmaßnahmen an.