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 2018/2019
Übungsblatt 8

Termin: 08.01.2019 um 12:00 Uhr

Aufgabe 17: (K) Kryptographische Hashfunktionen

a. Welche Eigenschaften besitzen Hashfunktionen bzw. kryptographische Hashfunktionen?

b. Geben Sie mindestens 2 mögliche Einsatzszenarien für (kryptographische) Hashfunktionen an.

c. Was versteht man unter dem Begriff *Kollisionsresistenz* im Zusammenhang mit kryptographischen Hashfunktionen?

d. Was versteht man unter dem Merkle-Damgard-Prinzip? Wird dieses z.B. bei Hashfunktionen wie MD5 angewendet?

Aufgabe 18: (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. Bei der Authentisierung von Nutzern findet eine 1:1-Verifikation statt. Nennen Sie ein Beispiel, bei dem eine 1:N-Verifikation erforderlich ist/sein könnte? (Tip: Fingerabdruck)

c. Sie sind ein Sicherheitsverantwortlicher in einem Unternehmen. Ihre Mitarbeiter benötigen auf Dienstreisen, auch aus Internet-Cafes heraus, Zugriff auf interne Ressourcen. Welchen Mechanismus zu einer möglichst sicheren Benutzerauthentisierung schlagen Sie der Unternehmensleitung vor? Begründen Sie ihre Antwort und zeigen Sie dabei Angriffsmöglichkeiten auf andere Mechanismen auf.

d. Welchen Vorteil bieten zur Absicherung von Remote-Zugängen Smartcard- und OTP-Token-basierte Lösungen? Welche(n) große(n) Nachteil(e) haben diese?

e. Betrachten Sie eine Web-Applikation. Zur Nutzerauthentisierung werden Passwörter eingesetzt, die 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.