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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2015/2016
Übungsblatt 9

Abgabetermin: 19.01.2016 bis 12:00 Uhr

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

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (über Uniworx als **Einzelabgabe**). Während des Semesters werden vier Übungsblätter ausgewählt, korrigiert und bewertet. Bei vier als korrekt bewerteten Lösungen (mind. 75% der erreichbaren Punkte) erfolgt ein Bonus von zwei Drittel Notenstufen auf die Klausurnote, bei nur drei oder zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer Drittel Notenstufe.

Bei Fragen zu Übungsaufgaben sowie generellen Anregungen, Verbesserungsvorschlägen, ... zum Übungsbetrieb wenden Sie sich bitte per Email an **`uebung-itsec@lrz.de`**.

Aufgabe 25: (H) Kryptographische Hashfunktionen (10 Punkte)

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?

e. Erstellen Sie eine einfache Tabelle. Nennen Sie vier verschiedene Hash-Algorithmen (außer MD5, Whirlpool) und geben deren verwendete Blockgröße, deren resultierende Digest Size (Länge des Hashes) und die Rundenzahl an.

f. Geben Sie für einen der in der vorherigen Aufgabe genannten Algorithmen einen möglichen Angriff an und beschreiben dessen Ablauf in Stichpunkten.

Aufgabe 26: (H) Authentisierung (8 Punkte)

In der Vorlesung haben Sie sich mit grundsätzlichen Möglichkeiten zur Authentisierung auseinander gesetzt, sowie sich mit dem Ablauf durch verschiedene Mechanismen abgesicherter Kommunikation zwischen Alice und Bob beschäftigt.

a. Als grundsätzliche Möglichkeiten zur Authentisierung sind *Wissen*, *Besitz* und *Persönliche Eigenschaften* bzw. eine Kombination dieser Faktoren möglich. Oftmals werden bei der Authentisierung aber noch weitere Aspekte einbezogen. Nennen und erläutern Sie mindestens zwei solcher Aspekte.

b. Bei einem biometrischen Verfahren werden zunächst in einer Initalisierungsphase die biometrischen Merkmale erfasst, um sie später beim Authentisierungsvorgang mit den aktuell gemessenen vergleichen zu können. Da es aufgrund meist äußerer Einflüsse und Messungenauigkeiten zwangsläufig zu Abweichungen dabei kommt, spielen Fehlerraten eine Rolle. Nennen und erläutern Sie zwei dieser Fehlerraten. Welche Rate, wenn Sie besonders hoch ist, ist aus Security-Perspektive gefährlicher? Begründen Sie Ihre Antwort knapp.

c. Sie sind Sicherheitsverantwortlicher in einem Unternehmen und sollen verschiedene am Markt erhältliche biometrische Systeme vergleichen. Wie Sie in der vorherigen Aufgabe gesehen haben, könnten Sie hierfür die von den Herstellern angegebenen Fehlerraten vergleichen? Ist das ihrer Meinung nach ausreichend oder wäre die Betrachtung der im Zusammenhang mit biometrischen Systemen oftmals genannten Equal Error Rate (EER) sinnvoller? Erläutern Sie diese an einem kurzen, selbstgewählten Beispiel.

d. Im Vorlesungsskript in Kapitel 10, Folie 43 wurde ihnen exemplarisch die Verwendung von Hash-Funktionen zur Authentisierung in Kombination mit einem symmetrischen Verschlüsselungsverfahren, das zusätzlich die Vertraulichkeit sicherstellen soll, erläutert. Erstellen Sie eine Skizze, die den Ablauf des Austauschs der Nachricht M plus einem berechneten Hash zwischen Alice und Bob unter Verwendung eines asymmetrischen Verschlüsselungsverfahrens darstellt.

Aufgabe 27: **(K)** Schlüssellängen

a. Wie lange dauert es mit einem gegebenen Rechner (3GHz, ca. $3 * 10^6 \frac{\text{Schlüssel}}{\text{s}}$) einen symmetrischen Schlüssel der Länge 56 Bit / 128 Bit mittels Brute Force zu brechen?

b. Wie lange benötigt man, um mit der genannten Maschine einen 4096 Bit langes RSA Modul zu brechen?

c. Wie würde sich die Existenz eines DNA- oder Quantencomputers auf die Sicherheit von DES, AES und RSA auswirken?