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 2014/2015
Übungsblatt 10

Abgabetermin: 20.01.2015 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.

Aufgabe 23: **(H)** Kryptographische Hashfunktionen & Geburtstags-Paradoxon (5 Punkte)

a. Wie definiert man im Allgemeinen kryptographische Hashfunktionen und geben Sie *mindestes* zwei mögliche Einsatzszenarien für Hashfunktionen an

b. Wie in der Vorlesung gezeigt müssen mindestens 23 Personen in einem Raum anwesend sein, so dass mit einer Wahrscheinlichkeit von 50% wenigstens 2 von ihnen am selben Tag Geburtstag haben. Formulieren Sie eine kurze Beweisskizze.

c. Wieviele Hashes (Länge 96 Bits) aus nicht identischen Input-Werten muss man demnach durchschnittlich berechnen, bevor es zu einer Kollision kommt?

Aufgabe 24: **(H)** Authentisierung & HMAC & X.509v3 (11 Punkte)

In der Vorlesung haben Sie sich mit grundsätzlichen Möglichkeiten zur Authentisierung auseinander gesetzt, außerdem sogenannte Hashed MACs kennengelernt, sowie sich allgemein mit Zertifikaten 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. Im Vorlesungsskript in Kapitel 8, 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. Skizzieren Sie den analogen Ablauf des Austauschs der Nachricht M zwischen Alice und Bob unter Verwendung eines asymmetrischen Verschlüsselungsverfahrens.

d. Beschreiben Sie in eigenen Worten den grundsätzlichen Ablauf eines Hashed-MAC-Verfahrens. Was sichert die äußere Hash-Funktion genau? Nennen Sie jeweils einen Vorteil und Nachteil vom HMAC gegenüber einem asymmetrischen digitalen Signaturverfahren.

e. Nennen und erläutern Sie mindestens 4 Felder, die ein X.509v3-Zertifikat aufweist.

f. Oftmals werden zur zweifelsfreien Identifikation einer Entität, z.B. eines Servers oder Nutzers, Zertifikate eingesetzt. Nennen und erläutern Sie mindestens 4 Aufgaben einer Certificate Authority (CA).

Aufgabe 25: (H) Needham-Schroeder (4 Punkte)

In der Vorlesung haben Sie das Authentisierungsprotokoll Needham-Schröder unter Verwendung eines symmetrischen Verschlüsselungsverfahrens kennengelernt.

a. Skizzieren Sie den Nachrichtenfluss der zum Verbindungsaufbau benötigten Pakete zwischen Alice und Bob bei Verwendung einer asymmetrischen Variante des Needham-Schröder-Protokolls. Den beiden Kommunikationspartnern sei hierfür der öffentliche Schlüssel K_T eines einer vertrauenswürdigen Instanz T bekannt. T kennt andererseits die öffentlichen Schlüssel aller Beteiligten (K_A für Alice, K_B für Bob).

b. Die symmetrische Protokollvariante von Needham-Schröder besitzt eine bekannte Schwäche für Replay-Attacken bei bekanntem Session-Key. Erläutern Sie das Problem im Detail. Welche Möglichkeiten gibt es, um die Ursache dieses Problems zu lösen?