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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2009/2010
Übungsblatt 6

Abgabetermin: 09.12.2009 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben benötigen Sie eine Rechnerkennung für unsere Praktikums Infrastruktur. Um diese zu erhalten, melden Sie sich bitte über die Vorlesungs Webseite zum Übungsberieb an.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email, in der Vorlesung oder vor der Übung). Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen 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 14: (H) Kryptographische Hashfunktionen & Geburtstags-Paradoxon

a. Wie definiert man im Allgemeinen kryptographische Hashfunktionen und geben Sie 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 aus nicht identischen Input-Werten muss man demnach durchschnittlich berechnen, bevor es zu einer Kollision kommt?

Aufgabe 15: (T) Nostradamus-Angriff gegen Hashfunktionen

Gegen Hash-Funktionen, die nach dem Merkle-Damgard Prinzip konstruiert sind, lassen sich spezielle Kollisionsangriffe konstruieren, die scheinbar die Kenntnis einer Information beweisen, die zu diesem Zeitpunkt eigentlich noch garnicht vorhanden sein kann. Dies lässt sich zu einem Angriff ausnutzen, bei dem zukünftige Dinge scheinbar vorausgesagt werden können.

Aufgabe 16: (H) Needham-Schroeder

a. In der Vorlesung wurde das Needham-Schroeder Protokoll unter Verwendung von symmetrischer Verschlüsselung behandelt. Skizzieren Sie den Nachrichtenfluss der zum Verbindungsaufbau benötigten Pakete zwischen Alice und Bob.

b. Skizzieren Sie den Nachrichtenfluss der zum Verbindungsaufbau benötigten Pakete zwischen Alice und Bob bei Verwendung von asymmetrischer Verschlüsselung.

c. Die symmetrische Variante des Needham-Schroeder Protokolls besitzt eine bekannte Schwäche für Replay-Atacken bei bekanntem Session-Key. Erläutern Sie das Problem und beheben Sie dessen Ursache!