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 2010/2011
Übungsblatt 6

Abgabetermin: 15.12.2010 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 15: (H) Kryptographische Hashfunktionen

a. Was versteht man unter dem Merkle-Damgard-Prinzip?

b. Erstellen Sie eine Tabelle. Nennen Sie 5 verschiedene Hash-Algorithmen (außer MD5, Whirlpool) und geben deren verwendete Blockgröße, Digest Size und Rundenzahl an.

c. Nennen Sie für einen der in der vorherigen Aufgabe genannten Algorithmus einen möglichen Angriff an und beschreiben diesen in Stichpunkten.

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

Aufgabe 16: (K) 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.
Es wurden 2008 insgesamt 12 PDF-Dokumente veröffentlicht, die jeweils unterschiedliche Gewinner der zu diesem Zeitpunkt bevorstehenden US-Präsidentenwahl nannten, aber alle denselben Hashwert aufwiesen.