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 2008/2009
Übungsblatt 9

Abgabetermin: 14.01.2009 bis 14:00 Uhr

Achtung: Die schriftlichen Lösungen aller mit H gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben. Während des Semesters werden drei Übungsblätter korrigiert. Bei drei richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 17: (K) SSL

Gegeben sind zwei SSL-VPNs, die Pakete auf der Ebene 2 bzw. 3 über Ethernet tunneln. Die MTU des Netzes berägt 1500 Bytes. Nehmen Sie an, dass die getunnelten IP-Pakete eine Payload von

a. 15 Byte

b. 1480 Byte

besitzen. Wie groß ist der Overhead der durch SSL gesicherten Daten im Vergleich zu den ungesicherten Paketen?

Aufgabe 18: (H) IPSec

IPSec verwendet intern 64 Bit lange Sequenznummern, übertragen werden aber lediglich die 32 niederwertigsten Bits. Erläutern Sie, wie IPSec in diesem Fall Replay Angriffe erkennen kann!