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 7

Abgabetermin: 10.12.2008 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 14: (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!

Aufgabe 15: (K) X.509

a. Erstellen Sie mit Hilfe von OpenSSL eine X.509 Certificate Authority (CA) mit der Lebensdauer von 10 Jahren!

b. Erzeugen Sie ein Public/Private Key Pair. Signieren Sie den Public Key mit Hilfe ihrer CA. Das Zertifikat soll 1 Jahr gültig sein.

c. Lassen Sie sich die Details ihres Zertifikates anzeigen.

d. Konvertieren Sie ihr Zertifikat in das PKCS Format.

e. Entfernen Sie das Passwort aus ihrem Schlüssel.

f. Widerrufen Sie das Zertifikat.