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 7

Abgabetermin: 16.12.2009 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 (per Email, in der Vorlesung oder vor der Übung) abzugeben. Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei zwei oder einer richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 17: (H) Biometrie 2009

Biometrie ist in aller Munde. Analysten erwarten ein starkes Wachstum in diesem Bereich innerhalb der nächsten Jahre. Die Nutzer erwarten Bequemlichkeit und höhere Sicherheit bei Finanztransaktionen und Bezahlvorgängen. Doch wo Chancen sind, sind auch Risiken.

a. Im Zusammenhang mit Biometrie sind die folgenden Begriffe relevant: Biometrisches Merkmal, Biometrisches Verfahren und Biometrisches System. Erläutern Sie die Begriff und geben Sie bei den Merkmalen mindestens drei praxistaugliche Beispiele an

b. Welche Anforderungen sollten im Allgemeinen biometrische Merkmale erfüllen? Wie sieht die Realität aus?

c. In der Vorlesung wurde ein allgemeines Vorgehensmodell im Zusammenhang mit Biometrie beschrieben. Skizzieren Sie dieses Modell

d. Welche Angriffsszenarien existieren im Bereich der Biometrie. Zeigen Sie wirksame Abwehrmechanismen auf.

Aufgabe 18: (H) 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. Welche grundsätzlichen Ansätze existieren für den Widerruf eines Zertifikats? Widerrufen Sie Ihr Zertifikat.