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 7

**Abgabetermin:** 12.01.2011 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

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

a. Nennen Sie mindestens 5 grundsätzliche Anforderungen an ein biometrisches System?

b. Wie wird die Leistungsfähigkeit eines biometrischen Systems im Allgemeinen gemessen?

## Aufgabe 18: (H) HMAC und Needham-Schroeder

Der HMAC mit 64 Bit Schlüssellänge wird wie in der Vorlesung definiert, berechnet. Gegeben sei eine Hashfunktion $H(x)$ und die 8 Byte langen hexadezimalen Konstanten

$$\mathrm{ipad} = 3636363636363636$$
$$\mathrm{opad} = 5C5C5C5C5C5C5C5C$$

Im Verlauf eines Protokolls soll ein 128-bit langer Parameter P ausgetauscht werden, der mit dem HMAC gesichert werden soll.

a. Gegeben sei der HMAC-Schlüssel $k = 9A45B7FE149BCE60$ und als Hashfunktion $H(x)$ der MD5 mit 128 Bit Ausgabelänge. Berechnen Sie den $\mathrm{HMAC}_k(P)$ für den Parameter $P = 000102030405060708090A0B0C0D0E0F$. Benutzen Sie für die notwendigen MD5 Berechnungen die folgende Tabelle:

| Eingabe $x$ (hex) | Ausgabe MD5$(x)$ (hex) |
|---|---|
| 0x1BAF81D154AD3D5600010203040506070809 0A0B0C0D0E0F | 0xA339A0A2E397F5D59FFECED63B32B4FC |
| 0x1B7381D122AD3D5600010203040506070809 0A0B0C0D0E0F | 0x398A7DE773C25BE09AF3425D02EB216C |
| 0x1B7381C822AD3D5601020304050607080 90A0B0C0D0E0F00 | 0xB9BFB2425097EE76B17C7AB7299F38D1 |
| 0x73DF81D154AD3D5600010203040506070809 0A0B0C0D0E0F | 0xB239A0A2E397F5D59FFECED63B32755D |
| 0x737381D122AD3D5600010203040506070809 0A0B0C0D0E0F | 0x88D37DE773C25BE09AF3425D02EB218C |
| 0x737399C822AD3D5601020304050607080 90A0B0C0D0E0F00 | 0xA23FB2425097EE76B17C7AB7299F3444 |
| 0xAC3881C822AD3D5601020304050607080 90A0B0C0D0E0F00 | 0xA95BBB4FF0A7511D07DC5CA6ACA6BE2E |
| 0xAC7381C822ADF8560001020304050607080 90A0B0C0D0E0F | 0x0898721134D8E73D7F0209244CFC733F |
| 0xAC7393B143ADF8560001020304050607080 90A0B0C0D0E0F | 0x58460D74328B15CC0E1B1FCF811E1621 |
| 0xC619EBA248C7923C0898721134D8E73D7F0209244CFC733F | 0xA4167961D793AE17467720AB1C636951 |
| 0xC619EBF623542A340898721134D8E73D7F0209244CFC733F | 0xDCB9C8C90936A7F26DC40C5403334AC8 |
| 0xC63AD4F623542A340898721134D8E73D7F0209244CFC733F | 0x36165CCD748C4F0DA3CD51D83A5EA2BE |
| 0xBB19EBA248C7923CB9BFB2425097EE76B17C7AB7299F38D1 | 0xB2167961D748AE17467720AB1C636425 |
| 0xBB59EBF623542A3458460D74328B15CC0E1B1FCF811E1621 | 0x14DFC8C90936A7F26DC40C54033388C3 |
| 0xBB3AD4F623542A340898721134D8E73D7F0209244CFC733F | 0x54AB5CCD748C4F0DA3CD51D83A5ECC8B |
| 0xFE19EBA248C7923CA339A0A2E397F5D59FFECED63B32B4FC | 0x125388B1D748AE17467720AB1C9476D3 |
| 0xFE59EBF623542A3458460D74328B15CC0E1B1FCF811E1621 | 0xFF33236AF936A7F26DC40C540940ABE1 |
| 0xFE5D3AF623542A34B239A0A2E397F5D59FFECED63B32755D | 0xCC325CCD748C4F0DA3CD51D83A19DA1F |

b. Nennen Sie jeweils einen Vorteil und Nachteil vom HMAC gegenüber einem asymmetrischen digitalen Signaturverfahren.

c. In der Vorlesung wurde das Needham-Schroeder Protokoll unter Verwendung symmetrischer Verschlüsselung erläutert. Skizzieren Sie den Ablauf unter Verwendung asymmetrischer Verschlüsselung.

d. Ein Angriff auf das Needham-Schroeder Protokoll ist die Lowe-Attacke. Beschreiben Sie diese in Stichpunkten. Kann dieser Angriff verhindert werden?

## Aufgabe 19: (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.

Erstellen Sie für die Abgabe der Hausaufgabe ein Protokoll, aus dem Kommandozeilenaufrufe und -ausgaben hervorgehen!