Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2016/2017
Übungsblatt 9

Abgabetermin: 24.01.2017 bis 12:00 Uhr

Aufgabe 20: (K) Kerberos

Ein weitverbreitetes Protokoll zur Benutzerauthentisierung ist Kerberos. Beschreiben Sie den Ablauf sowie den konkreten Aufbau der ausgetauschten Nachrichten anhand des folgenden Beispiel-Szenarios:

a. Sie kommen um 08:00 Uhr in die Arbeit und loggen sich mit Ihrem Nutzernamen *bsp26395* und zugehörigem Passwort *3z!fG7qiT* ein. An welche an Kerberos-beteiligte Komponente werden diese Informationen übermittelt? Wie sieht die zugehörige Nachricht aus?

b. Die Antwort, die Sie auf Ihre erste Nachricht in Teilaufgabe a) erhalten ist verschlüsselt. Welcher Schlüssel wurde hierzu verwendet? Welche Informationen werden in dieser Antwort-Nachricht übertragen?

c. Sie arbeiten gerade an einem Text-Dokument, welches Sie nun ausdrucken wollen. Die Steuerung des Druckers erfolgt über einen dedizierten Print-Server. An welche Kerberos-Komponente müssen Sie Ihre Druck-Anfrage übermitteln und welche Informationen enthält diese? Welchen Inhalt hat die entsprechende Antwortnachricht?

d. Welche Schritte sind abschließend zu durchlaufen, damit Ihr Dokument ausgedruckt wird?

Aufgabe 21: (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 und erstellen sie ein Certificate Signing Request (CSR).

c. Signieren Sie den Public Key mit Hilfe ihrer CA. Das Zertifikat soll 1 Jahr gültig sein.

d. Lassen Sie sich die Details ihres Zertifikates anzeigen.

e. Welche grundsätzlichen Ansätze existieren für den Widerruf eines Zertifikats? Erläutern Sie diese und widerrufen Sie Ihr Zertifikat.