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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2015/2016
Übungsblatt 10

Abgabetermin: 26.01.2016 bis 12:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (über Uniworx als **Einzelabgabe**). Während des Semesters werden vier Übungsblätter ausgewählt, korrigiert und bewertet. Bei vier als korrekt bewerteten Lösungen (mind. 75% der erreichbaren Punkte) erfolgt ein Bonus von zwei Drittel Notenstufen auf die Klausurnote, bei nur drei oder zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer Drittel Notenstufe.

Bei Fragen zu Übungsaufgaben sowie generellen Anregungen, Verbesserungsvorschlägen, ... zum Übungsbetrieb wenden Sie sich bitte per Email an **`uebung-itsec@lrz.de`**.

Aufgabe 27: **(K)** Kerberos (4 Punkte)

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 28: (H) X.509 (6 Punkte)

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.

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

Aufgabe 29: (H) LetsEncrypt (10 Punkte)

In der vorheringen Aufgabe haben Sie selber eine Certificate Authority (CA) erstellt und damit ein Zertifikat unterschrieben. Ein Problem von SSL ist allerdings, dass diese selbst unterschriebenen Zertifikate bei anderen Benutzern eine Warnung auslösen, da diese, wenn Sie nicht den Public-Key ihrer CA verteilen, die Authentizität des Zertifikats überprüfen können. Bis auf wenige Ausnahmen war das Erstellen eines von einer „vertrauenswürdigen“ CA unterschriebenen Zertifikats bisher umständlich und teuer. Das soll durch das, unter anderen von Mozilla und der EFF unterstützte, Projekt LetsEncrypt `https://letsencrypt.org`, anders werden.

a. Beschreiben Sie **kurz** den Aufbau der von LetsEncrypt eingesetzten Zertifikatskette.

b. Beschreiben Sie allgemein mindestens drei Möglichkeiten („plugins“ genannt) mit dem LetsEncrypt-Client ein signiertes Zertifikat erzeugen zu lassen. Nennen Sie zu jeder Methode mindestens einen Vor- und einen Nachteil.

c. Beschreiben Sie konkret, wie sie das in der vorherigen Aufgabe (28b) erstellte CSR verwenden können um ein von LetsEncrypt unterschriebenes Zertifikat zu bekommen.

d. Beschreiben Sie allgemein mindestens drei Vor und Nachteile der von LetsEncrypt erstellten/unterschriebenen Zertifikate.

e. LetsEncrypt verwendet Certificate Transparency. Beschreiben Sie kurz Certificate Transparency Logs und nennen Sie mindestens einen Vor und Nachteil.