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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2011/2012
Übungsblatt 9

Abgabetermin: 18.01.2012 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben benötigen Sie eine Rechnerkennung für unsere Praktikumsinfrastruktur. Um diese zu erhalten, melden Sie sich bitte über die Vorlesungswebseite zum Übungsbetrieb an.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per **E-Mail** an die Adresse **uebung-itsec_AT_lrz.de** oder schriftlich vor der Übung). Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen 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.

Aufgabe 20: (H) Needham-Schroeder & X.509v3

In der Vorlesung wurde das Authentisierungsprotokoll Needham-Schröder unter Verwendung eines symmetrischen Verschlüsselungsverfahrens erläutert.

a. Skizzieren Sie den Nachrichtenfluss der zum Verbindungsaufbau benötigten Pakete zwischen Alice und Bob bei Verwendung von asymmetrischer Verschlüsselung. Den Kommunikationspartnern sei der öffentliche Schlüssel K_T von Trent T bekannt. Trent kennt andererseits die öffentlichen Schlüssel aller Beteiligten (K_A für Alice, K_B für Bob).

b. Die symmetrische Protokollvariante von Needham-Schröder besitzt eine bekannte Schwäche für Replay-Attacken bei bekanntem Session-Key. Erläutern Sie das Problem und beheben Sie dessen Ursache!

c. Oftmals werden zur zweifelsfreien Identifikation einer Entität, z.B. eines Servers oder Nutzers, Zertifikate eingesetzt. Nennen und erläutern Sie mindestens 5 Aufgaben einer Certificate Authority (CA).

d. Das LRZ betreibt eine CA für das Münchner Wissenschaftsnetz, welche in die Zertifizierungshierarchie des DFN integriert ist. Skizzieren Sie den Zertifizierungspfad eines LRZ-Nutzerzertifikates unter Berücksichtigung des Sicherheitsniveaus *Global*. Fügen Sie zusätzlich den Wert des öffentlichen Schlüssels des derzeit gültigen Wurzelzertifkates Ihrer Lösung hinzu.

Aufgabe 21: (H) Network-Security & 802.1X

Eine sehr einfache, aber dennoch sehr effiziente Möglichkeit Netztraffic zu separieren stellt der Einsatz von Virtual LANs (VLANs) dar.

a. Erläutern Sie knapp den Aufbau eines VLAN-Tags. Welche Aufgabe besitzt die Priorisierung. Welche Prioritätseinstufung schlagen Sie für Video- bzw. IP-Telefonie vor?

b. Die Kommunikation zwischen den Systemen derselben Broadcast Domain ist jedoch ungefiltert möglich. Eine Filterung dieser Kommunikation ist durch sogenannte Virtual Access Lists (VACLs) oder durch Private VLANs (PVLANs) möglich. Erläutern Sie stichpunktartig diese Verfahren.

c. 802.1X ist ein in WLAN- und VLAN-Infrastrukturen häufig verwendeter Network Access Control-Mechanismus. Sie benötigen in einem Besprechungsraum am LRZ Internet-Zugang und schließen Ihr Notebook an eine der zur Verfügung stehenden Netzdosen an. Welche erste Nachricht sendet der Supplicant, wenn der Authenticator nicht bekannt ist?

d. Welche Gefahr besteht beim Senden der Identitätsinformationen des Supplicants an den Authenticator?

e. Skizzieren Sie die weitere Kommunikation zwischen Supplicant, Authenticator und Authentication Server generell. Was ist zwingende Voraussetzung bei Verwendung von EAP-TLS?

f. Welchen Vorteil hat eine zusätzlich durchgeführte MAC-Authentifizierung?