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 9

Abgabetermin: 26.01.2011 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 abzugeben (per Email, in der Vorlesung oder 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 22: (H) Diffie-Hellman

a. Berechnen Sie die Werte der relevanten Größen, die beim Schlüsselaustausch zwischen Alice und Bob mit Hilfe des Diffie-Hellman Verfahrens entstehen. Wie lautet der ausgetauschte Schlüssel, wenn Alice den Schlüsselaustausch initiiert und als Wert für die Primzahl 23 sowie 5 als Wert für die Primitive Wurzel vorgibt. Gehen Sie davon aus, dass die gewählte Zufallszahl von Alice 6 und die von Bob 15 ist.

b. Versetzen Sie sich in die Lage von Eve, die die Kommunikation von Alice und Bob mithört. Kann Eve den ausgetauschten Schlüssel mit den ihr bekannten Werten berechnen?

c. Beschreiben Sie einen möglichen Angriff auf das Diffie-Hellman Schlüsselaustauschverfahren.

Aufgabe 23: (H) IPSEC Protokollkombinationen

Wie in der Vorlesung beschrieben, können die Protokolle AH und ESP entweder unabhängig voneinander oder in Kombination eingesetzt werden. Dabei ist zu unterscheiden, ob eines oder beide kommunizierenden Endsysteme selbst IPSEC-fähig sind oder ob so genannte Security Gateways eingesetzt werden. In der Vorlesung wurden bereits ausgewählte Kombinationen und deren charakteristische Eigenschaften besprochen

a. Gegeben sei ein Quellsystem mit der IP-Adresse 10.1.1.1 mit Security-Gateway 10.1.1.254 und ein Zielsystem 10.10.1.1 mit Security-Gateway 10.10.1.254. Für die Kommunikation soll

- AH soll im Tunnel-Mode zwischen den Security-Gateways
- ESP im Transport-Mode zwischen den Endsystemen

verwendet werden. Geben Sie für alle beteiligten Systeme exemplarische Inhalte aller relevanten Security Associations an; gehen Sie dabei davon aus, dass die Vertraulichkeit über AES-Verschlüsselung und die Integritätssicherung über MD5-Prüfsummen sicher gestellt werden soll.

b. Geben Sie, analog zu den Folien im Vorlesungsskript, den Inhalt des Pakets an. Gehen Sie dabei von einem zu übertragenden IPv4-Datagramm aus. Geben Sie für alle relevanten Header-Felder korrekte Werte an.