Technische Universität München
Informatik VIII
Netzarchitekturen und Netzdienste
Prof. Dr.-Ing. Georg Carle

Dipl.-Inf. Ali Fessi

Übungen zur Vorlesung „Netzsicherheit“
Übungsblatt 1, WS08/09

Abgabe: Mi. 29. Oktober 2008
Besprechungstermin: Mi. 5. November 2008

Anmeldung bzw. Email-Liste:
Für die Übung ist eine Anmeldung erforderlich. Die Anmeldung kann unter folgender Web-Seite erfolgen: http://www.net.in.tum.de/de/lehre/ws0809/vorlesungen/network-security/

Abgabe: Es sind insgesamt 6 Übungsblätter vorgesehen. Ein Blatt kann von bis zu 2 Studenten gemeinsam bearbeitet werden. Der Termin für die Abgabe ist Mittwochs in der Vorlesung.

Scheinvergabe:
Zum Scheinerwerb ist hinreichend:
• Regelmäßige und aktive Teilnahme an den Übungen
• 75% der Aufgaben werden sinnvoll bearbeitet. „Sinnvoll“ heißt, dass es sichtbar ist, dass sich zu der Aufgabe aufgabenrelevante Gedanken gemacht worden sind.
• Jeder Teilnehmer muss mindestens ein Mal eine Aufgabe vorrechnen.
Bei Bachelor/Master-Studenten kann die Veranstaltung „Netzsicherheit“ bei erfolgreicher Teilnahme an der Übung mit 5 ECTS statt 4 ECTS berechnet werden.

Aufgabe 1: Sicherheitsbedrohungen und Sicherheitsdienste

Gegeben sei eine Client-Server Architektur mit einem potentiellen Angreifer auf dem Datenpfad.
Der Angreifer hat die Möglichkeit folgende Angriffe durchzuführen:

- Nachrichten abhören
- Nachrichten verfälschen
- Nachrichten verzögern
- Nachrichten löschen

Gehen Sie davon aus, dass bestimme Mechanismen für dieses Protokoll zur Verfügung stehen, die folgende Sicherheitsdienste erfüllen:

- Vertraulichkeit
- Datenintegrität

(Solche Mechanismen werden im Laufe der Vorlesung bekannt, z.B. Verschlüsselungsalgorithmen und kryptographische Hash-Funktionen)

a) Welche der oben genannten Angriffe können schon mit den vorhandenen Sicherheitsmechanismen verhindert werden?
b) Begründen Sie, warum die Vertraulichkeit der Daten nicht garantieren kann, dass die Daten unbemerkt verändert werden können.

c) Damit die oben genannten Sicherheitsanforderungen an diesem Protokoll vollständig erfüllt werden, müssen zusätzlich noch weitere Aufgaben erledigt werden. Beschreiben Sie hierfür eine Maßnahme, die es dem Server ermöglicht, eine Verzögerung einer Nachricht von über 45 Sekunden zu erkennen.
d) Beschreiben Sie eine Maßnahme, die es dem Server ermöglicht, zu erkennen:
   - ob eine Nachricht von einem Angreifer gelöscht wurde.
   - ob eine Nachricht von einem Angreifer wiedereingespielt wurde (”Replay Attack“).

Aufgabe 2: Brute-Force Angriffe auf Passwörtern

Gegeben sei ein passwort-basiertes Authentisierungsverfahren mit einem Passwort der Länge 8 Bytes. Mit einem Brute-Force Angriff versucht ein Angreifer systematisch sich mit allen möglichen Passwörtern zu authentisieren.

Angenommen, ein Authentisierungsversuch dauert 1 µs und der Authentisierungsserver ist nicht zustandsbehaftet, d.h. er merkt sich die Geschichte der Authentisierungsversuche bei einem Benutzer nicht.
a) Unter der Annahme, dass ein Benutzer ein Passwort mit nur kleinen Buchstaben verwendet und dass alle Passwörter gleichwahrscheinlich sind, wie lange braucht ein Angreifer durchschnittlich, um sich erfolgreich zu authentisieren?
b) Berechnen Sie den durchschnittlichen Aufwand für die Authentisierung falls für das Passwort zusätzlich große Buchstaben, Ziffern und 31 weitere ASCII Sonder-Zeichen in Frage kommen (man spricht hier von „starken Passwörtern“) und dass wieder alle Passwörter gleich wahrscheinlich sind.

Aufgabe 3: Ping-of-Death

Die Applikation ”ping“ wird verwendet, um die Erreichbarkeit von Hosts im Internet (beispielsweise ein öffentlicher Web-Server) zu überprüfen. Das Programm schickt dabei eine ICMP ”echo request“ Nachricht zu diesem Host. Der Host antwortet in der Regel mit einer ICMP ”echo reply“ Nachricht.

Viele Firewalls in Firmennetzwerken werden allerdings so konfiguriert, dass sie ICMP-Nachrichten blockieren. Einer der Gründe für diese Maßnahme ist der sogenannte ”Ping-of-Death“ Angriff.

a) Recherchieren Sie im Internet und beschreiben Sie kurz diesen Angriff.
b) Ist dieser Angriff spezifisch für ICMP oder sind solche Angriffe mit anderen Transport-Protokollen, z.B. UDP, auch möglich? Begründen Sie Ihre Antwort.
c) Beschreiben Sie mögliche Gegenmaßnahmen, um diesen Angriff zu vermeiden.

Aufgabe 4: Netwerk-„Sniffer“ am Beispiel von Wireshark

Um diese Aufgabe durchzuführen, installieren Sie den Paket-Sniffer Wireshark[1] und machen Sie sich mit seiner Funktionalität vertraut, z.B. mit den Definitionen von ”Capture Filters“.
Starten Sie Ihren Internet-Browser und beobachten Sie den HTTP-Verkehr mit Wireshark. Achten Sie dabei auf die ausführlichen Informationen, die Wireshark anzeigt, über die Daten, die auf verschiedenen Schichten übertragen werden, z.B. IP, TCP, HTTP.
a) Beschreiben Sie kurz, welche Sicherheitsrisiken sich ergeben, wenn solche Anwendungen Daten im Internet unverschlüsselt versenden.
c) Öffnen Sie eine Webseite mit dem HTTPS-Protokoll. Ist es noch möglich den Inhalt der Anwendungsschicht zu lesen? Welche Information zeigt Wireshark in diesem Fall über die Anwendungsdaten?
d) Die Verbindung zu einem Webserver basiert auf das Transport-Protokoll TCP (Schicht 4)

[1] Wireshark ist sowohl für Linux- als auch Windows-Systeme verfügbar (siehe http://www.wireshark.org/)

und das Anwendungsprotokoll HTTP (Schicht 7). Die ersten drei TCP Nachrichten werden mit:

- SYN (Client → Server)
- SYN-ACK (Server → Client)
- ACK (Client → Server)

bezeichnet und werden zum Verbindungsaufbau mit dem Webserver verwendet.

Suchen Sie diese Pakete mit Wireshark aus und geben Sie an, welche der sogenannten „Flags“ SYN, ACK, RST und FIN bei diesen 3 Paketen gesetzt sind und welche nicht.