RUHR-UNIVERSITÄT BOCHUM
Fakultät für Elektro- & Informationstechnik
Lehrstuhl für Kommunikationssicherheit
Christof Paar, Benedikt Gierlichs, Ahmad-Reza Sadeghi

5. Übung zur Vorlesung Netzwerksicherheit

Diese Übung beschäftigt sich mit einigen Aspekten von Secure SHell (SSH).

Aufgabe 1 - Allgemeines

a) Welche Dienste bietet SSH?

b) Nennen Sie einige Funktionen, die SSH nicht zur Verfügung stellt.

c) Was bedeutet *port forwarding* und wie funktioniert es?

d) Skizzieren Sie die Architektur von SSH-2 und geben Sie die wichtigsten Komponenten von SSH an.

Aufgabe 2 - Schlüsselaustausch

Während der Initialisierungsphase einer SSH-Server-Applikation werden verschiedene Schlüsselpaare für kryptographische Funktionen erzeugt.

a) Wofür und für wen werden diese Schlüssel verwendet?

b) Skizzieren Sie den Ablauf des SSH-2 Schlüsselaustauschprotokolls.

Aufgabe 3 - Ein wenig Praxis

Für diese Aufgabe sollen Sie eine durch einen SSH-Tunnel geschützte Verbindung mit dem Webserver des Hosts `waldorf.crypto.rub.de` aufbauen und die Datei *image.jpg* herunterladen. Hierzu verbinden Sie sich mit dem SSH-Server (ebenfalls `waldorf.crypto.rub.de`) auf Port 2323 unter der Verwendung der Benutzername - Passwort - Kombination, die Sie in Übung 3 durch die Wörterbuch-Attacke erfahren haben.

a) Mit welchen Parametern müssen Sie den SSH-Client starten?

b) Welcher Verschlüsselungsalgorithmus wird zur vertraulichen Kommunikation verwendet?

c) Welcher Signaturalgorithmus wird verwendet?

d) Welchem Zweck dient das Passwort, das Sie bei der Anmeldung am SSH-Server eingeben? Wie wird dieses Ziel erreicht?

e) Was ist der Inhalt der JPEG-Datei?