

**Aufgabenblatt 9**  
**(NUR FÜR ULI-STUDENTEN)**

Abgabetermin: Mittwoch, 29. Juni 2005, 12:00 Uhr MEZ (per E-Mail an  
mathias.kutzner@hpi.uni-potsdam.de)

Bearbeitung: für jede Aufgabe separates Blatt mit Name und Matrikelnr.  
(wichtig!)

Themen: Sicherheit, HTTP  
maximale Punktzahl: 17

**Aufgabe 1: WEP-Verschlüsselung**

**5 Punkte**

Warum gilt WEP als unsicher ? Beschreiben Sie wie unbefugte Personen in den Besitz des geheimen WEP-Schlüssels gelangen können (Angriffsszenario). (3 Punkte)

Erklären Sie den Unterschied von WPA zu WEP und begründen Sie, warum WPA als sicherer angesehen wird. Ist WPA wirklich so sicher ? (2 Punkte)

**Aufgabe 2: Public- Key- Verfahren**

**4 Punkte**

Ein Administrator möchte, dass regelmäßig ein automatisches Backup eines Netzwerkrechners durchgeführt wird. D.h. ein entfernter Login muss ohne Passwortabfrage erfolgen. Wie könnte er ein Backup über SSH mit Public- Key-Authentifizierung durchführen? Beschreiben Sie, was auf den jeweiligen Rechnern mit den Keys gemacht wird und warum.

**Aufgabe 3: HTTP**

**8 Punkte**

1) Schreiben Sie einen einfachen HTTP Webserver in Java oder Perl. Dokumentieren Sie Ihr Programm ausführlich.

- Benutzer muß die Portnummer des Servers angeben
  - Nur GET-Methode implementieren
  - Zusätzliche Request Header Felder können ignoriert werden
- (6 Punkte)

2) Welche nutzerbezogenen Daten lassen sich aus HTTP-Server Logfiles gewinnen ? (2 Punkte)