Christian Schindelhauer

Freiburg, den 09. Juli 2007
Besprechung 05. Juli 2007

Übungen zur Vorlesung

Systeme-II

Sommer 2007

Blatt 11

AUFGABE 27:
DNS verwendet UDP anstatt TCP. Geht ein DNS-Paket verloren, wird es nicht automatisch wiederhergestellt. Führt dies zu einem Problem und wenn ja, wie wird es gelöst?

AUFGABE 28:
Einige E-Mail-Systeme unterstützen das Header-Feld *Content Return:*. Es bestimmt, ob der Nachrichteninhalt im Falle einer Nichtzustelung zurückgesendet werden muss. Gehört dieses Feld in den Umschlag oder in den Header? Begründen Sie!

AUFGABE 29:
Kategorisieren Sie die folgenden fünf Bedrohungen eines Netzwerks gemäß der verletzten Sicherheitsziele und der Bedrohungstypen aus der Vorlesung!

- Trojaner-E-Mail, welche Transaktions-IDs für Online-Banking ausspioniert
- Netzwerkrouter, der Paketinhalte analysiert und kategorisiert
- Denial-of-Service Angriff auf einen Webserver
- Systemadministrator, der Log-Dateien in der Netzwerkadministration manipuliert
- Notebook-User, der unerlaubt das W-LAN seines Nachbarn benutzt

AUFGABE 30:
Pretty Good Privacy (PGP) ist ein Programm zur Verschlüsselung von Daten. Es benutzt ein Schlüsselpaar, d.h. einen öffentlichen Schlüssel, mit dem jeder die Daten für den Empfänger verschlüsseln kann, und einen geheimen privaten Schlüssel, den nur der Empfänger besitzt. Der verwendete Verschlüsselungsalgorithmus basiert dabei auf dem RSA-Verfahren. Machen Sie sich mit dem Programm vertraut und führen Sie folgende Schritte durch:

- Laden Sie sich eine PGP Software aus dem Internet, diese finden Sie unter http://www.pgpi.com.
- Erzeugen Sie sich ein Schlüsselpaar.
- Tauschen Sie Schlüssel mit Teilnehmern der Übungsgruppe aus. Schicken Sie eine signierte und verschlüsselte E-Mail an alle Tauschpartner.