Übungsblatt 7

Aufgaben vom 6.5.2010

Diese Aufgaben sind für die nächsten 2-3 Wochen gedacht und erfordern auch die Bereitschaft, sich zu Hause in die Materie einzuarbeiten

Aufgabe 1 - SSL / X509

Generieren Sie SSL Client Zertifikate und authentisieren Sie sich damit gegenüber einer Webapplikation.

Setzen Sie einen Webserver so auf, das er Zugriffe nur mit gültigen SSL Client Zertifikat (von einer bekannten Root CA signiert) akzeptiert.

Lesen sie dann in ihrer WebApplikation (zum Beispiel einem CGI oder einem PHP Script) das ‘Subject’ aus dem SSL-Client Zertifikat und geben sie es aus.

Wenn Sie ein Client-Zertifikat brauchen: Siehe Aufgabe 3

Aufgabe 2 - EMail

Informieren Sie sich über Vor- und Nachteile von X.509 S/MIME und PGP im Zusammenhang mit E-Mail.

Erzeugen Sie sich je einen X.509 und einen PGP Key und tauschen Sie vertrauliche und signierte Mails mit einer anderen Übungsgruppe aus.

Wenn Sie ein X509 Client-Zertifikat brauchen: Siehe Aufgabe 3

Aufgabe 3 - PKI / CA

Schauen Sie sich das Projekt cacert.org an. Hier können Sie kostenlose X509 Zertifikate bekommen.

Aufgabe 4 - VPN

Richten Sie eine VPN Verbindung zwischen zwei Rechnern ein. Entweder auf Basis von IPSec oder auf Basis von OpenVPN.

Authentisieren Sie die VPN Verbindung mit Zertifikaten

.