Hochschule RheinMain, Prof. Dr. Martin Gergeleit

Rechnernetze & Telekommunikation
SoSe 2020
LV 2142

Übungsblatt 9

Bearbeiten Sie diese Aufgaben bitte **vor** Beginn Ihrer Praktikumsgruppe und halten Sie Ihre Ergebnisse **schriftlich** in einem Protokoll Ihrer Versuche fest. Die nötigen Informationen über ACLs erhalten Sie aus den Vorlesungen (https://video2.cs.hs-rm.de/course/5/lecture/78/, Rechnernetze und Telekommunikation > 10. Netzwerksicherheit Teil 3). Mehr Details finden Sie auch in meiner Online-Vorlesung speziell zur PKI https://video2.cs.hs-rm.de/course/81/lecture/651/)

Zu Beginn werden Einzelne vom Praktikumsleiter stichprobenartig gebeten elektronisch abzugeben. Die Bearbeitung der Fragen bildet mit eine Grundlage der Bewertung.

Die Fragen werden anschließend in der Praktikumsgruppe interaktiv besprochen und vorgeführt.

Vorbemerkungen und Hinweise

Für diesen Versuch benötigen Sie lediglich den SSH-Zugang zum login1.cs.hs-rm.de und einem E-Mail-Client wie z.B. Mozilla Thunderbird auf einem beliebigen System.

Achten Sie darauf, bei der Eingabe der Angaben zu den Zertifikaten **korrekte Angaben** zu machen und darauf, dass diese Angaben beim erstellten **root-Zertifikat und dem Mail-Zertifikat gleich sind**, weil sonst das Signieren fehlschlägt.

Sichere Kommunikation (E-Mail) mit Zertifikaten und S/MIME

Da immer mehr sicherheits- und datenschutzrelevante Informationen über das öffentliche Internet übertragen werden, ist es zunehmend von Interesse, die Sicherheit der Teilnehmer und ihrer Informationen gegen Dritte zu sichern. Im Bereich von E-Mails hat sich der Standard S/MIME (Secure Multipurpose Internet Mail Extension) durchgesetzt, eine Erweiterung des Internet-Standards MIME, der die Verschlüsselung und das Signieren von E-Mails und die Authentifizierung des Absenders ermöglicht.

Das Verschlüsseln und/oder Signieren von E-Mails basiert auf X.509-Zertifikaten, die durch eine Public Key Infrastruktur (PKI) bereitgestellt werden um Anwender einwandfrei zu identifizieren. Mit Hilfe eines solchen Zertifikats, das den öffentlichen Schlüssel des Benutzers beinhaltet sowie eines S/MIME-fähigen E-Mail-Clients kann der Anwender jetzt E-Mails digital signieren und/oder verschlüsseln. Alle aktuellen E-Mail-Clients unterstützen diese Funktionen heute, häufig fehlt allerdings die zu ihrer Nutzung erforderliche PKI in den Organisationen.

In diesem Praktikumsversuch sollen Sie die grundsätzlichen Mechanismen lernen, auf denen eine PKI beruht und mit denen z.B. sichere E-Mail implementiert werden kann.

Aufgabe 9.1: Erzeugen eines selbst-signiertes Root Zertifikats

Legen Sie zunächst ein eigenes Unterverzeichnis für Ihre Zertifikatsverwaltung an und erzeugen Sie die darin die notwendigen Verzeichnisse und Dateien:

```
mkdir CertAdm
cd CertAdm
mkdir newcerts private
touch index.txt
echo '01' > serial
cp ~gergelei/RN/openssl.cnf .
```

Erzeugen Sie ein 2048 Bit RSA Schlüsselpaar für Ihre Root-CA:

```
openssl genrsa -aes128 -out private/CAkey.pem 2048
```

Welche Rolle spielt das symmetrische AES128 Verfahren hier?

Erzeugen Sie nun das selbst-signiertes Root Zertifikat.

```
openssl req -new -x509 -days 1460 -key
    private/CAkey.pem -out CAcert.pem -config openssl.cnf
```

Lassen Sie sich das Zertifikat in lesbarer Form anzeigen:

```
openssl x509 -in CAcert.pem -noout -text
```

Aufgabe 9.2: Erzeugen eines persönlichen Zertifikats

Erzeugen Sie ein eigenes Schlüsselpaar mit (wählen Sie dabei eine andere Passphrase für Ihren privaten Schlüssel als bei der Root-CA):

```
openssl genrsa -aes128 -out private/Mykey.pem 2048
```

Erzeugen Sie eine Zertifikatsanforderung:

```
openssl req -new -key private/Mykey.pem
    -out MyReq.pem -config openssl.cnf
```

Tragen Sie Ihren Namen unter „Common Name“ und Ihre gültige „Email Address“ ein. Welche Rolle spielt die Konfigurationsdatei openssl.cnf? Diskutieren Sie insbesondere die X.509 Extensions und die Unterschiede zwischen selbst signierten CA Zertifikaten und User Zertifikaten.

Ihr Trustcenter signiert jetzt die Anforderung:

```
openssl ca -notext -in MyReq.pem -out Mycert.pem
    -config openssl.cnf
```

Welchen privaten Schlüssel setzen Sie hier ein?

Lassen Sie sich Ihr neues Zertifikat in lesbarer Form anzeigen. Geben Sie Ihren öffentlichen RSA Schlüssel (e, N) an!

Wandeln Sie Ihr Zertifikat, Ihren privaten Schlüssel und der Root-CA-Zertifikat vom PEM-Format in das PKCS#12-Format um:

```
openssl pkcs12 -export -in Mycert.pem -inkey
    private/Mykey.pem -certfile CAcert.pem -out
    Mycert.p12 -name "My Certificate"
```

Aufgabe 9.3: Übersicht

Erstellen Sie eine Übersichtszeichnung, in der Sie die bisher erzeugten Datei-Objekte mit den jeweiligen Schlüsseln (root/persönlich, public/private) und ihre Beziehungen darstellen.

Aufgabe 9.4: Mail-Verschlüsselung mit S/MIME

Importieren Sie das Root-CA Zertifikat sowie Ihr Zertifikat einschließlich privatem Schlüssel in Ihr Mail-Programm (z.B. Mozilla Thunderbird). Schicken Sie Ihrem Übungsgruppenleiter eine mit dem S/MIME-Verfahren signierte Email.

Was müsst noch getan werden, damit der Empfänger eine solche signierte Email überprüfen kann?

Warum können Sie jetzt keine verschlüsselte Email schicken?