4. Übungsblatt

Übung Peer-to-Peer-Systeme und Sicherheit (SS2009)

26. Juni 2009
Abgabetermin: Fr. 10.7.
Übungstermin: Do. 16.7.

Dipl.-Inform. Heiko Niedermayer
Lehrstuhl für Netzarchitekturen und Netzdienste
Technische Universität München

Regeln:
Es sind insgesamt 5 Übungsblätter mit je 10 Punkten vorgesehen. Ein Blatt kann von 3 Studenten gemeinsam bearbeitet werden. Für die Übungscredits wird erwartet, dass Aufgaben für 30 Punkte sinnvoll bearbeitet wurden und dass 1x erfolgreich eine Aufgabe vorgerechnet worden ist.

Aufgabe 1 (2 Punkte) Skype-Sicherheit
Die Sicherheit von Skype haben wir nur extrem kurz behandelt (s. Kapitel 1). In dieser Aufgabe gehen wir ein paar Fragen dazu nach. Begründen Sie dabei jede Antwort.

a) Die zentrale Komponente bei Skype sind die Login-Server. Kann Skype auch ohne Login-Server sichere Authentisierung bieten?
b) Ein weiterer Sicherheitsmechanismus bei Skype ist das Programm als Closed-Source zu betreiben und dabei auch durch einige Massnahmen externes Debugging massiv zu erschweren. Was erreicht Skype dadurch?
c) Ist Closed-Source für den sicheren Betrieb einer Skype-artigen Software notwendig? Geben Sie einen Grund oder ein Gegenbeispiel an.

Aufgabe 2 (2 Punkte) Authentisierung
In dieser Aufgabe geben wir ein kryptographisches Protokol an, welches beidseitige Authentisierung vorsieht. Für das Protokoll ist anzugeben, woran die Entitäten im Protokollablauf die Authentisierung des gegenüber feststellen können. Des Weiteren ist das Protokol unsicher und es soll ein Angriff angegeben werden. Der Angreifer soll dabei die übliche Mächtigkeit in der Netzsicherheit haben, d.h. er soll keine Kryptographie brechen können, aber beliebig im Netzwerk Nachrichten lesen, versenden, faken und abfangen können.

Vorwissen: S ist TTP. Jeder Teilnehmer X hat einen gemeinsamen Schlüssel kXS mit S gemeinsam.
Es sei kab = Nb.

```
A -> B: Na,A
B -> S: Na,A,B,{Nb}kBS
S -> A: B,{Na,Nb}kAS
A -> B: {Nb}kab
```

Aufgabe 3 (2 Punkte) Authentisierung
Gehen Sie wie in Aufgabe 2 vor. Das Protokoll ist diesmal ein anderes.

Vorwissen: S ist TTP und kennt zu jedem Teilnehmer X den entsprechenden aktuellen Public Key PK_X.
Es sei kab = hash(Na,Nb).

```
A -> S: Na,A,B
S -> A: PK_B,Enc_PK_A(SigS(Na,A))
A -> B: Enc_PK_B(Na,A,SigS(Na,A))
B -> A: Nb,{Na}kab
```

Aufgabe 4 (2 Punkte) Verständnisfragen
Ein paar Fragen, die mit dem Wissen aus der Vorlesung beantwortbar sein sollten.

a) Kryptographische Identitäten sollen die Authentisierung einfacher machen. Wenn kryptographische Identitäten verwendet werden, sind dann trotzdem Certificate Authorities notwendig? Wenn ja, wofür. Wenn nein, Nichtbedarf begründen.
b) Welche Rolle spielt Vertrauen bei der Verteilung von Schlüsseln?
c) Warum machen Zfone oder SSH im Baby Duck-Modell nicht einfach Authentisierung per konventionellem Authentisierungsprotokoll – welches Problem müssen Sie umschiffen?

Aufgabe 5 (2 Punkte) Sybil-Angriff
In der Vorlesung wurde der Sybil-Angriff vorgestellt.

a) Warum ist der Sybil-Angriff fatal für die Sicherheit eines Peer-to-Peer-Netzwerks?
b) Wie würde ein Sybil-Angriff auf Ebay aussehen und wie könnte der Angreifer profitieren?