P2P - Theorie Aufgabe 7

Arne Link (1582381), Lars Fritche (1691285)
Gruppe 14 (S217/103)

February 10, 2014

1 Aufgabe 7.1 Safebook

1.1 Matryoshka

Matryoshkas sind konzentrische Kreise um einen Knoten, auch 'core' genannt, der eben jenen Knoten beschützen soll. Als 'shell' werden dabei, die Knoten bezeichnet, die sich in den konzentrischen Kreisen befinden. Der 'inner shell' ist der erste Kreis um den Knoten und besteht aus direkten Kontakten des 'core'.

Das Besondere am 'inner shell' ist, dass die Knoten die zu ihm gehören, die Daten des 'core' verschlüsselt bei sich speichern. Aus diesem Grund werden die einzelnen Knoten auch 'mirrors' genannt, da sie ein Duplikat der Daten des 'core' enthalten. Der 'outer shell' ist der vom 'core' am weitesten entfernte konzentrische Kreis. Er dient als Zugang, der Daten-Anforderungen an den 'core' leitet, weswegen seine Knoten auch als 'entry points' bezeichnet werden. Die Kreis zwischen 'inner' und 'outer' werden als 'intermediate shell' bezeichnet.

1.2 Purpose of Matryoshkas

Matryoshkas werden für jeden neuen Knoten erzeugt und erzeugen eine 'trust' Struktur, da nur Knoten miteinander verbunden sind, die einander vertrauen. Dabei speichern die Knoten der 'inner shell', die Daten des 'core', sofern sie protected oder public sind und können so auch verbreitet werden, wenn der nicht mit dem Netzwerk verbunden ist.

1.3 Overlays

Das erste Overlay sind die matryoshkas deren Funktion es ist ein Netzwerk um einen Knoten aufzubauen, dessen einzelne Teilnehmer ihren Nachbarn vertrauen.

Das zweite ist die P2P-Schicht, die sich um lookup-Dienste im OSN kümmert.

1.4 Profile lookup

Die Abfrage nach Daten wird über eine rekursive Anfrage gestartet. Wird der Knoten gefunden, der für den 'lookup key' verantwortlich ist, schickt dieser eine Liste von 'entry points' der matryoshka zurück. An einen 'entry point' aus der Liste wird dann eine Anfrage gestellt, die bis zu einem 'mirror' weitergeleitet wird. Von dort aus werden die verschlüsselten Daten über den inversen Pfad zurückgeschickt. Möchte ein User einem anderen eine Kontaktanfrage senden, so wird diese ebenso gesendet wie Datenabfragen. Sollte der andere User annehmen, weist er dem Anfragenden ein 'trust level' zu und schickt ihm einen Key, mit dem er die Daten aus den 'mirrors' entschlüsseln kann.

Ein wichtiger Aspekt ist der TIS, mit dem garantiert wird, dass ein Knoten immer das selbe Pseudonym und Knotenid erhält und somit 'Sybil' und 'impersonation' Attacken, die in anderen DHTs ein ernst zu nehmendes Problem darstellen, verhindert werden.

Darüber hinaus besitzt man durch die 'mirrors' die Möglichkeit Daten auch dann bereitstellen zu können, wenn der Core sich abgemeldet hat (solange ein 'mirror' noch online ist)