Internet and Web Applications, Übung 7

Henry Haustein

Aufgabe 1: VoIP and NAT

(a) Session Traversal Utilities for NAT (STUN, englisch für Werkzeuge zum Durchkreuzen von NATs) ist ein einfaches Netzwerkprotokoll, um das Vorhandensein und die Art von Firewalls und NAT-Routern zu erkennen und direkte Verbindungen zwischen Geräten, welche sich hinter einer NAT-Firewall befinden, aufzubauen. Damit ist es Geräten, welche hinter bestimmten Typen von NAT-Firewalls betrieben werden, möglich direkte bidirektionale Verbindungen zwischen den Endknoten aufzubauen. Beispiele für die Anwendung von STUN sind SIP-Telefone und Computer-Programme in Heimnetzwerken.

(b) STUN dient dazu, die Informationen wie die öffentliche IP-Adresse und Port-Nummer für den direkten Kontaktaufbau zwischen zwei Endgeräten, den "Clients", welche sich normalweise nicht direkt erreichen können, zu ermitteln um dann in Folge und unabhängig von STUN, den Clients mit diesen Informationen die direkte Kontaktaufnahme zu ermöglichen. STUN wird unter anderem bei der IP-Telefonie (v. a. im Zusammenhang mit SIP) und bei Online-Spielen von Spielekonsolen eingesetzt.
STUN wurde in RFC 3489 definiert und stand damals noch für englisch Simple traversal of UDP through NATs. Aufgrund der gemachten Erfahrungen und neuen Definitionen aus anderen RFCs wurde STUN dann überarbeitet und in englisch Session Traversal Utilities for NAT umbenannt (RFC 5389). Dabei wurde STUN als Framework neu definiert, und alle Funktionen bis auf die Basisfunktionalität verschwanden; dafür wurde allerdings definiert, wie Erweiterungen möglich sind.
Ein in der Funktion ähnliches Protokoll stellt TURN dar, die Abkürzung steht für englisch Traversal Using Relays around NAT, welches im Gegensatz zu STUN sich eines externen, im öffentlichen Internet befindlichen Relay-Server bedient, um so eine Verbindung zwischen Clients mit einem direkten Kommunikationskanal aufzubauen. Dies erlaubt auch Kommunikationen wo die direkte Verbindung von Endgeräten untereinander durch bestimmte, restriktive NAT-Firewalls blockiert werden. Der Nachteil ist, dass der normalerweise verschlüsselte Datentransfer über den TURN-Server laufen muss und diese Anbindung bei vielen Verbindungen einen Flaschenhals darstellt.

https://de.wikipedia.org/wiki/Session_Traversal_Utilities_for_NAT

Aufgabe 2: Offer/Answer Model

The use of SDP with SIP is given in the SDP offer answer RFC 3264. The default message body type in SIP is application/sdp.

- The calling party lists the media capabilities that they are willing to receive in SDP, usually in either an INVITE or in an ACK.
- The called party lists their media capabilities in the 200 OK response to the INVITE.

A typical SIP use of SDP includes the following fields: version, origin, subject, time, connection, and one or more media and attribute.

- The subject and time fields are not used by SIP but are included for compatibility.
- In the SDP standard, the subject field is a required field and must contain at least one character, suggested to be `s=-` if there is no subject.
- The time field is usually set to `t = 00`. SIP uses the connection, media, and attribute fields to set up sessions between UAs.
- The origin field has limited use with SIP.
- The session-id is usually kept constant throughout a SIP session.
- The version is incremented each time the SDP is changed. If the SDP being sent is unchanged from that sent previously, the version is kept the same.
- As the type of media session and codec to be used are part of the connection negotiation, SIP can use SDP to specify multiple alternative media types and to selectively accept or decline those media types.

The offer/answer specification, RFC 3264, recommends that an attribute containing `a = rtpmap`: be used for each media field. A media stream is declined by setting the port number to zero for the corresponding media field in the SDP response.

https://www.tutorialspoint.com/session_initiation_protocol/session_initiation_protocol_the_offer_answer_model.htm