NAT Traversal

draft-kaufman-rtcweb-traversal-00

Matthew Kaufman

8 June 2011

Drawbacks of a Full ICE Implementation

- Limits Adaptability
- Hampers Innovation
- Unneccesary Cost in some Cases

Summary of approach

- Expose primitives for sending and receiving STUN connectivity tests
- Do NOT implement ICE internally

- Primitives are:
  - Send Test
  - Receive Test at Far End (and reply)
  - Receive Reply

Before Test

- Assume a PeerConnection object
- Must support:
  - Get (or set) local STUN credentials
  - Client SHOULD generate the credentials itself and provide an API for read-only access
- Credentials are transmitted out-of-band

Send Test (Initiator)

- Client provides a function to send a STUN connectivity test
  - Parameters:
    - far address and port number
    - the far username and password
    - additional ICE attributes to be included in the STUN Binding Request message.
  - This function causes a single STUN RFC 3489 [RFC3489] Binding Request with short-term credentials to be sent to the far address from the initiating client.
  - Username concatenation is performed as per ICE 7.1.2.3.
- MUST rate limit transmission of these requests
- MUST NOT allow the user of the API to specify or examine the transaction ID for this request
  - prevents spoofing of successful replies by an attcking host.
- STUN request is safe: very unlikely to simulate other traffic
- STUN request is sent from the exact same IP address and port that the PeerConnection object will use for subsequent media traffic

Receipt of Test (Responder)

- Upon receipt of a STUN Binding Request with valid credentials
  - SHOULD automatically generate and send the STUN transaction response
    - If it does not, an API for sending the transaction response MUST be provided
  - Triggers a callback function or event that delivers:
    - attribute/ value pairs received in the Binding Request
    - locally derived (reflexive) address from which the Binding Request was received

Receipt of Response (Initiator)

- Upon receipt of a valid STUN transaction response
  - Triggers a callback function or event that delivers:
    - attribute/value pairs received in the response
    - one of which is the reflexive address.
  - Adds the now-verified address to the “Transmit Whitelist”
    - This is a list of socket addresses to which sending of media is now permissible. The client MUST NOT allow media to be sent to any address/port combination that has not been added to the Transmit Whitelist.
  - Note: Response MUST be ignored if the receivedSocketAddress does not match the socket address to which the matching transaction ID was sent (ICE 7.1.3.2)

Capabilities of Proposed Model

- ICE in Javascript
- Server-Based ICE
- STUN-Only
- Non-ICE

Security Considerations

- “Transmit Whitelist”
  - prevents a client from sending media to an endpoint which has not properly responded to a STUN request.
- Client must:
  - **internally generate** the transaction ID
  - not allow it to be explicitly set **or read back**
  - This prevents spoofing of the STUN test replies.