

ICE and RTP DoS

draft-rosenberg-mmusic-rtp-denialofservice

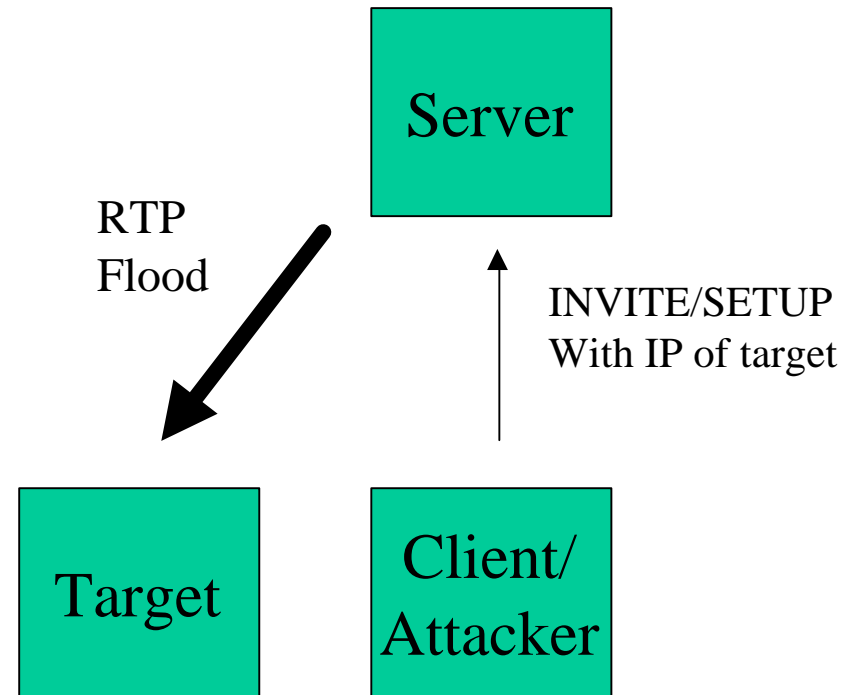
draft-rosenberg-sipping-ice

Jonathan Rosenberg

dynamicsoft

The DoS Problem

- Attacker sends SIP INVITE or RTSP SETUP to server
- IP for RTP is target
 - Source IP in RTSP
 - SDP in SIP
- Server sends media to target



Scope of Problem

- Easily launched by script kiddies
- Nearly infinite amplification
 - Particularly effective with multimedia servers
- All it needs is a server that accepts many simultaneous calls
- With RTSP, “send only to RTSP source” limits it a bit
 - NAT makes it worse – opens the attack to anyone behind your NAT
- With SIP, its really bad – no similar checks

Mitigation

- Authentication
 - Can help identify the sender of the attack
 - Can't prevent the attack
 - Many services have weak enrollment, so authentication doesn't help
 - Web signups
- Don't send what's not wanted
 - Before sending RTP, check that someone is actually listening at the target address
 - Requires a request/response mechanism to the RTP ports
 - Mechanism must not be amenable to attacks itself
 - That's ICE!

Proposal

- This security consideration needs to be documented, along with solutions
 - Part of revision of RFC 2326
 - An additional document that updates offer/answer
- Further discussion is needed on whether ICE is right for RTSP
- Seems right for SIP

ICE

Problem Statement

- We still don't have a good answer for NAT traversal in SIP!!
- That is clear from nat-scenarios
 - Tons of cases
 - Best solution in each case depends on network topology, business issues, etc.
- Lots of components
 - STUN, TURN, MIDCOM, RSIP, etc.
- How can we expect interop or reliability?

Solution: Interactive Connectivity Establishment (ICE)

- ICE is a methodology for NAT traversal
 - Makes use of STUN, TURN, RSIP, MIDCOM
 - Entirely resident within the clients
- ICE explains how to use the other protocols for NAT traversal
- ICE Properties
 - Always will find a means for communicating if one physically exists
 - Always finds the lowest latency communications path
 - Always finds the communication path cheapest for the service provider
 - Does not require any knowledge of topology, NAT types, or anything

Basic ICE Algorithm

- Client obtains addresses
 - Local interfaces
 - UNSAF protocols
 - VPNs
- Client lists all of them in an offer
- Answerer tests connectivity to each of those
 - Connectivity test uses peer-to-peer STUN
- Connectivity test may yield more addresses
- Answer provides all its addresses (local interfaces, UNSAF, VPNs + STUN derived addresses)
- Offer performs the same connectivity check
- Highest priority address is used
- May require several iterations

History

- Presented at IETF 56
- Revision submitted for IETF 57
- SIPPING agrees they want this, but they recognize that ICE is purely an offer/answer/SDP issue
 - May be used for RTSP as well
- So, the SIPPING group and TSV AD s felt it would best be done in mmusic
 - Would be amenable to a charter revision to add
- SIP usage cases would be done in sipping
- Proposal: take ICE as a work item and make it applicable to SIP and RTSP