Fixing IP Leaks related to WebRTC – DHT

WebRTC - Western Illinois University Graduate Thesis

Dennis McMeekan: December 2020

# Abstract

As previously discussed in a survey describing security concerns related to a WebRTC based application, it is vital that IP Leaks be masked and covered in such a way that a client does not get punished for using the application. “Any two devices talking to each other directly via WebRTC, however, need to know each other’s real IP addresses” [1]. This will allow for the other client, and more frightening, a 3rd party application the ability to detect and misuse the original client’s real IP address. Although this may be apparent currently, our committee has come under the impression that through a similar fashion as the Tor browser, a Distributed Hash Table server representation may be a solve to the issue.

This would obviously require vigorous and intensive testing and implementation to acquire this sort of product, but this paper will at least touch the surface and dive into how exactly this would be possible and the types of action that would need to occur.

# Current Approach

# New Approach

# Prerequisites

# Implementation

# Benefits

# Sources

ExpressVPN. “How to use the WebRTC leak checker,” *ExpressVPN.* Accessed on: Dec. 4, 2020. [Online]

Available: <https://www.expressvpn.com/webrtc-leak-test>