WebRTC Covert Channels by Image Filtering

An Abstract of a

Thesis Presented to the

Department of Computer Science

Western Illinois University

In Partial Fulfillment

of the Requirements for the Degree

Master of Computer Science

By

Dennis McMeekan

May, 2021

ABSTRACT

“WebRTC is an open-source web-based application technology, which allows users to send real-time media without the need for installing plugins” [1]. This type of technology has become a main-stay in all industries, and more specifically WebRTC being open-source has allowed for researchers and developers across the world to discover new advancements and heights of real-time communication without prior installations or requirements. Although this has provided a great source of real-time communication, there are still concerns with this being a relatively new application. This study will look further into data integrity regarding these types of applications, along with briefly discussing the issue of solving IP leaks through a distributed hash table. To further develop this topic, a simple WebRTC application has been created with the purpose of sending a bit through a covert channel based on a delay in data being received from one peer to another, focusing on the bitrate, round-trip-time, framerate, and error rate. Furthermore, this issue will then be mitigated to ensure that individuals developing a WebRTC application can further prepare for defense against such attacks or misusage.

APPROVAL PAGE

This thesis by **Dennis McMeekan** is accepted in its present form by the Department of Computer Science of Western Illinois University as satisfying the thesis requirements for the degree Master of Computer Science.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Chairperson, Examining Committee

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Member, Examining Committee

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Member, Examining Committee

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

WebRTC: Covert Channels by Image Filtering

A Thesis Presented to the

Department of Computer Science

Western Illinois University

In Partial Fulfillment

of the Requirements for the Degree

Master of Computer Science

By

Dennis McMeekan

May, 2021

ACKNOWLEDGMENTS

Grateful acknowledgment is extended to Dr. Binto George, thesis supervisor, and committee members Dr. Nilanjan Sen and Dr. Chunying Zhao for their valuable suggestions and guidance given in this thesis project.

TABLE OF CONTENTS

Acknowledgments . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ii

Table of Contents . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . iii

List of Tables . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . v

Chapter 1 – Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1

Chapter 2 – Background and Related Work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

2.1 Problem Statement . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 12

2.2 Security Concerns . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

2.2.1 Data Integrity . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

2.2.2 Covert Channels . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

2.2.3 IP Leaks . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

Chapter 3 – Research Methodology & Implementation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

3.1 Security Study. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

3.2 Open-Source Project Examples . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

3.3 WebRTC API . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

3.4 Image Filtering . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

3.5 Unsecure Prototype . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

3.6 Secure Prototype . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

Chapter 4 - Findings & Analysis of Data . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

Chapter 5 - Summary, Conclusions and Recommendations . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

5.1 Future Work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24

Appendices . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 26

1. Source Code . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

LIST OF TABLES

No. Title Page

I. Bureau of Prison Facilities Activated in last 5 years . . . . . . . . . . . . . . . . . . . . . . 16

II. Bureau of Prison Facilities in the Planning or Constructive Stage . . . . . . . . . . . 17

III. Federal Prisoner Population Projections (1996-2006) . . . . . . . . . . . . . . . . . . . . . . 25

IV. Iowa Prison System (as of July 1, 2000) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 25

**CHAPTER ONE**

**INTRODUCTION**

In a cultural and technology environment that is continuously evolving, real-time communication is more essential than ever for individuals to complete daily tasks such as school, work, and personal communication. “Live chat has become the leading digital contact method for online customers, as a staggering 46% of customers prefer live chat compared to just 29% for email, and 16% for social media” [2]. With the reach of internet to all points of the world, it is realistic to see that real-time calls between two or more individuals will be the main product for online communication methods. In recent years, WebRTC applications have been used to establish real-time communication between two or more peers. This product provides limitless advantages to web developers across the entire world, but with these advantages, there are also disadvantages. The main focus of this study is to determine the security factors that may be exploited with WebRTC and mitigating these issues. The emphasis for the research and project portion was data integrity related to covert channels, along with a brief survey on IP leaks. Data integrity is an issue because of WebRTC’s open-source model, clients hold the ability to alter the actual data that is being sent from one peer to another using the API provided. Specifically, the application can be altered to create covert channels via image filtering, a process that takes the video input, alters the data, and then outputs the video. This proves to be a problem, because having a secure data transfer from one individual to another is a vital process in application development. It was discovered that by implementing a delay in data transfer from one client to another, a bit can be sent and received based on this delay by the other client. This would provide the idea that data (messages) can be transferred secretly through clients without any control or knowledge by the administrator. There is a prevention method to prevent this from occurring,

which is implementing random delays on the server or administrative side. This will greatly increase the error rate due to the inability of each client to send and then sense the delay in data. These discoveries were mainly done using WebRTC’s API and different test elements such as the bitrate, round-trip-time, and framerate in an effort to determine the error rate. Beyond this, IP leaks is highly discussed as a security flaw with WebRTC applications, as in most cases the user’s public IP address is used directly. This is commonly addressed with the use of a VPN (Virtual Private Network), but in almost all cases this can be a costly effort and can be limited in the data limitations of the client.

In establishing an understanding of the vulnerabilities, a security study was conducted to look further into possible security flaws with WebRTC and real-life examples or discoveries of data integrity problems with these applications. Roughly in the past ten years, there have been a number of open-source examples that have been centered around WebRTC that focused on the altering of data. These were vital in providing a sense of direction on how to discover covert channels and altering/preventing data transformation. The most common way to develop a WebRTC application is using the open-source API implemented by the creators Google, with the two main languages of JavaScript and HTML5. To prove and further research, two prototypes have been created. An unsecure version, which focuses on creating a covert channel, delaying/sensing data, and then receiving a bit based on the delay. Finally, a secure prototype was created to combat this issue, implementing random delays to further increase the error rate at which the bit is being received.

**CHAPTER TWO**

**Background and Related Work**

This chapter focuses on the issue at hand as well as looking into research examples and open-source examples. This combination of work provides great insight into understanding and finding a route to combat and lead the way of thesis work.

**2.1 Problem Statement**

2.2 Security Concerns . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

2.2.1 Data Integrity . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

2.2.2 Covert Channels . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

2.2.3 IP Leaks . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

**References**

[1] NTT Communications (2015). *A Study of WebRTC Security*. Retrieved August 20, 2020

(<https://webrtc-security.github.io>)

[2] MacDonald, Steven (2021). *25 Reasons Live Chat Can Help You Grow Your Business in 2021*. Retrieved February 3, 2021

(<https://www.superoffice.com/blog/live-chat-statistics>)