RTCWEB
Internet-Draft
Intended status: Informational
Expires: December 24, 2012

D. York
Internet Society

June 22, 2012

Security Concerns For RTCWEB Congestion Control
draft-york-rtcweb-congestion-security-xx

Abstract

As the Real-Time Communication in WEB-browsers (RTCWEB) working group explores options for congestion control to ensure that browser-based voice, video and data communication do not overwhelm a network, care must be taken to ensure that the congestion controls have appropriate security mechanisms to prevent mis-use by potential attackers.

This document explores potential security concerns and attacks that could be made against congestion controls.

NOTE: While this document is in the form of an Internet-Draft, it has been created for the IAB/IRTF Congestion Control Workshop on July 28, 2012, and has NOT yet been submitted as an I-D. It is written in this style, though, with the intent that it may be submitted as an I-D in the future.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 24, 2012.

Copyright Notice

Table of Contents

1. Introduction

The Real-Time Communication in WEB-browsers (RTCWEB) working group is working to standardize protocols that can be used to enable interoperability between web browsers for interactive real-time communication using audio, video, chat, collaboration, games, etc.. See draft-ietf-rtcweb-overview [I-D.ietf-rtcweb-overview] for an overview of the goals of the overall RTCWEB initiative.

The RTCWEB working group is now exploring how best to provide "congestion control" along the lines described in RFC 2914 [RFC2914] and expanded upon for UDP in RFC 5405 [RFC5405]. The primary objectives are:

- Prevent the collapse of a network due to congestion.

- Provide a level of fairness to all traffic flows on the network.

It is expected that as RTCWEB is implemented in common web browsers the amount of real-time communication traffic could be quite substantial and thus the need for adequate congestion control is critical.

Security concerns for RTCWEB have already been well-documented in draft-ietf-rtcweb-security [I-D.ietf-rtcweb-security] and draft-ietf-rtcweb-security-arch [I-D.ietf-rtcweb-security-arch]. However, the potential addition of congestion control mechanisms introduces additional possible avenues of attack.

While some of these attacks may be adequately mitigated by security mechanisms already required for RTCWEB implementations, this document outlines these potential security concerns for discussion and consideration.

2. Potential Attacks Against Congestion Control Mechanisms

As no congestion control mechanism is yet defined for RTCWEB, the potential attacks below are hypothetical and are raised as questions to be discussed. Some of the proposed congestion control mechanisms may turn out not to be susceptible to some or all of these attacks. Other proposed mechanisms may be vulnerable. This document does not make assumptions about whether the congestion control mechanism might be implemented in the media stream, signaling stream or by some other means.

2.1. Denial of Service To An Individual User

An attacker may want to disrupt the communication flow from a specific user or set of users. This could be to target a specific user or to disrupt a certain set of communication exchanges.

Can the attacker maliciously modify congestion control signals in such a way that the traffic flow from a user or set of users is significantly degraded to the point where communication is no longer useful? Perhaps by tricking the sender into believing there is great congestion and introducing excessive latency? Or signaling to a RTCWEB endpoint that it repeatedly needs to switch to a different media codec? Or signaling to the target endpoint that there is simply too much congestion for any RTCWEB communication to occur?

2.2. Elevation of Service For An Individual User

Conversely, an attacker might want to give higher priority to a specific traffic flow (including his or her own) to the detriment of other users.

Can the attacker maliciously modify the congestion control signals so that a particular traffic flow can be given higher priority? Perhaps by signaling to all other RTCWEB streams that there is too much congestion?

2.3. Denial of Service For A Network

If there is a large volume of RTCWEB traffic on a given network and a congestion control mechanism ensures that the traffic does not overwhelm the network, an attacker may find that an easy way to perform a denial of service (DoS) against the entire network may be to simply remove all congestion control signals or convince all RTCWEB endpoints that there is no congestion.

Can an attacker maliciously modify the congestion control signals to strip out any such signaling? Or perhaps modify the congestion control signals in such a way that sending endpoints believe there is no congestion and that they can send at their highest available volumes?

2.4. Change of Communication Mode

RTCWEB communication is expected to allow multiple modes of communication, i.e. voice, video, chat, data collaboration, etc. A RTCWEB session between two users might involve all of the above. A congestion control mechanism could allow specification of which traffic flows receive priority and how the different flows are

addressed when faced with congestion. For instance, when congestion levels become too high, a video flow may be dropped while an audio or chat flow may continue.

Could an attacker maliciously modify congestion control signals to force such a downgrade? For one or both users?

3. Inter-Domain Considerations

A RTCWEB communication session is not expected to take place entirely within one network or administrative domain. It may take place across multiple networks or even more likely take place across the public Internet.

Can the confidentiality and integrity of the congestion control signals be ensured across all the various networks through which the session travels?

4. Next Steps

The potential attacks outlined here need to be further explored to determine if they are, in fact, valid attacks against potential RTCWEB congestion control mechanisms. Discussion needs to be held to understand if there are additional potential attacks beyond those listed here.

The potential attacks that are valid then need to be compared against the security mechanisms defined in draft-ietf-rtcweb-security [I-D.ietf-rtcweb-security] and draft-ietf-rtcweb-security-arch [I-D.ietf-rtcweb-security-arch] to understand whether or not the attacks may be mitigated or eliminated by already-required security mechanisms.

Any congestion control mechanisms brought for consideration to the RTCWEB working group need to indicate how they address these and other security considerations.

5. Security Considerations

This entire document is about security considerations.

6. References

6.1. Normative References

[RFC2914] Floyd, S., "Congestion Control Principles", BCP 41, RFC 2914, September 2000.

[RFC5405] Eggert, L. and G. Fairhurst, "Unicast UDP Usage Guidelines for Application Designers", BCP 145, RFC 5405, November 2008.

6.2. Informative References

[I-D.ietf-rtcweb-overview]
Alvestrand, H., "Overview: Real Time Protocols for Brower-based Applications", draft-ietf-rtcweb-overview-04 (work in progress), June 2012.

[I-D.ietf-rtcweb-security]
Rescorla, E., "Security Considerations for RTC-Web", draft-ietf-rtcweb-security-03 (work in progress), June 2012.

[I-D.ietf-rtcweb-security-arch]
Rescorla, E., "RTCWEB Security Architecture", draft-ietf-rtcweb-security-arch-02 (work in progress), June 2012.

[I-D.alvestrand-rtcweb-congestion]
Lundin, H., Holmer, S., and H. Alvestrand, "A Google Congestion Control Algorithm for Real-Time Communication on the World Wide Web", draft-alvestrand-rtcweb-congestion-02 (work in progress), April 2012.

Author’s Address

Dan York
Internet Society
Keene, N.H.
USA

Phone: +1-802-735-1624
Email: york@isoc.org