Reading Summary: How Secure and Quick is QUIC? Provable Security and Performance Analyses

Jakob Roberts - v00484900 - CSC 466

Mar 20, 2017

1 The Problem(s)

Please describe the problem(s) in your own words. Is the problem important at the time of paper publication, and how about now? Why?

The problem is that current encrypted connections are usually associated with high overheads and latency. QUIC hopes to decrease the latency while maintaining similar encryption standards. This paper goes into extreme depth(proofs) as to how QUIC stacks up in the security front.

2 Main Idea(s)

Please describe the main idea(s) in your own words. How is the idea different from the existing work at the time of paper publication? How does the idea impact the follow-on work till now?

The idea isn't much different, they are trying to compare security between protocols by providing a provable security analysis. The proofs associated with the analysis will give validity to the claims in security. At the time of paper publication, there have been other internet protocol alternatives, but in the paper they compare to TCP with TLS.

3 Major Strengths

Please list at least three most important things in this paper. Why do you think they were important at the time of paper publication? How about now?

They provide a great summary of what is listed in the paper in the introduction sections so you can get an understanding of what types of analysis were done. Despite all the complicated terminology, the authors spend a good deal of important time setting up information(sections 2, 3, 4, 5) relevant to the actual research sections(6, 7, 8) in order to help understand the relevance of the research done. In section 9, they actually talk about the results of well known attack types and how they would relate to QUIC, instead of doing a mathematical proof. They speak in the conclusion that QUIC has pitfalls, as would any performance based system.

4 Major Weaknesses

Please list at least three things you think may need further improvement in this paper. Has the improvement appeared in the follow-on work already?

Unfortunately the paper is not very friendly to people who are not already familiar with security related topics. In section 3 they describe naming conventions and set up mathematical assumptions, this means that whoever is reading the paper also needs to be well versed in the understanding of proof theory. Despite nicely having the sections separated. I feel like this paper could have been separated into multiple topics: one describing the mathematical proofs behind QUIC's security, and another more qualitative talking about the known attack vectors. I don't expect that these things to be improved upon.

5 Possible Improvement

Do you have some ideas of your own on this problem? Can you do something better or differently? How can you show that?

I would look at comparing QUIC to other up-and-coming internet protocol architectures and see how their performance compares. I don't think I could do anything better as it is out of my scope of knowledge.