Reaction to “Practical Comprehensive Bounds on Surreptitious Communication over DNS ”

1) Technical details (approach/technique) that you found novel/ Something specific you learned that you didn't know before

In this paper they first describe the tunneling attack through DNS, as well as mentioning several tools that can be readily used. This is a novel knowledge to me although the principle of the attacking is easy to understand.

Another thing I feel like interesting is that the authors didn’t try to identify all potential attack using automatic method. Instead of that, they only choose to use calculated upper bound to decrease the sample count need to be checked then do the remaining check manually. This method works pretty well in this case and I have to admit this method is also one thing I have learned from the paper.

2)Could I have done this work if I had the idea why or why not?

I think I am able to do the work in case I can find the chance to collect data from large party. The method they use in this paper is not hard to replicate.

3)Is there anything I could do to repeat or validate?

I think it would be possible for us to validate their method based on Clarkson’s network traffic.

4) What is my best idea for follow on work that I could personally do?

The author had validate their method based on some popular tunneling tools. The manual operation after the automatic process is also based on being familiar with the pattern used by some specific tool. However, I am still doubt whether the method will work for new patterns through DNS tunneling. I want to try the method against more pattern to validate its feasibility.

5)What is my best idea for follow on work that I'd like to see the authors do?

There are two following works I would like to see the author of this paper to do.

One is about the analysis to the “unknown” case mentioned in the result. It seems like this kind of query also contains some information and is possibly an unidentified tunneling method. I would like to see more analysis against this kind of query.

Another one is about the analysis of theoretical upper bound. The analysis gives me a feeling that this upper bound is too loose. I want to see more analysis that based on actual example which could tighten the upper bound.

6)Any logistical experimental lessons I learned?

No.

7)How does this compare to the other papers we read? Most similar? How different? Other comparisons?

This paper provides a novel idea of filtering out attacks that using other method is hard to identify. Even if it requires the assistance of manual processing. It is still a new and effective method that is different from other papers we have read before.

8)What is your biggest criticism of the paper?

I think the biggest problem of this paper is the inaccuracy of the data provided. In the paper the authors mentioned their methods of determining theoretical upper bound of information that can be conveyed. However, in practice they didn’t mention the actual data calculated from this theoretical upper bound. I feel like the authors should include this data in their paper to make the result more convincing.