This is a sample review for 660. You can use any editor for typesetting your review (Latex, notepad, etc.), but please convert your review into PDF before submitting. Note that reviews are due before the class. Please use the following format.

Sample Review:

Name: Amir Houmansadr
Class date: 01-23-2018
Paper title: RAINBOW: A Robust And Invisible Non-Blind Watermark for Network Flows

Summary: *[[Briefly introduce the paper, including the problem it studies, the core techniques they use, and some of the core results/findings of the paper. You do not talk about things you like or dislike about the paper here. 3-4 sentences should be enough. Also, do not copy paste from the paper :) Write the summary in your own words.]]*

The paper designs a new technique for correlating network flows, which they call RAINBOW. The core idea of RAINBOW is to slightly delay network packets in a way to modulate a secret signal, called the watermark signal, into the packet timings of network flows. The proposed technique is different from previous designs by being "non-blind", i.e., the traffic analysis parties use a side channel to communicate information about the flows they analyze. Through simulations and experiments on the Internet, the authors show that RAINBOW offers a significantly better correlation performance compared to previous designs.

Pros: *[[This is a list of things you liked about the paper. It may include things like the novelty of the idea, the significance of the results, a nice engineering work, good presentation/writing, advantages over previous work, etc.]]*

- I found the studied problem timely given the recent correlation attacks on anonymity systems. The proposed watermarking technique can improve the effectiveness of such attacks on anonymity systems, and therefore, are important to study.

- In addition to performing simulations, the authors evaluate the performance of their proposed technique by analytically modeling network traffic using stochastic processes and using hypothesis testing to derive analytical false positive and false negative rates. The analytical results mostly confirm the empirical results.

- The authors evaluate the invisibility of the proposed technique, showing that it is highly undetectable by two major statistical tests.

Cons: *[[This is a list of the weaknesses of the paper and things that you did not like, or think could have been better. Make sure your comments are not offensive to the authors! Think positive, and give constructive suggestions.]]*

- The authors do not perform experiments on the live Tor network (instead, on Planetlab).

- The paper's writing was rough at some points. I also suggest adding a clearer threat model section early in the paper. *[[Well, we will review papers accepted at top-tier conferences, so very likely you won't be complaining about writing or presentation!]]*

- The authors do not consider an active adversary (who continuously perturbs suspect traffic) in their threat model. I think an active adversary may be realistic in some real-world scenarios.

- The paper improves upon previous watermarking techniques by using a non-blind technique. The improvements make sense given that the new technique is non-blind, however, non-blind techniques are much less usable compared to blind techniques, as they require a side-channel between the watermarking entities.

- The invisibility evaluations do not give a theoretical guarantee on invisibility. The authors show that their technique is undetectable by two statistical tests (K-S test and entropy tests), but this does not prove invisibility against arbitrary classifiers. For instance, how about machine learning techniques?

Other comments: *[[Here you may include the less important comments you may have about the paper, or your questions/suggestions to the authors.]]*

- Looking at figure 10, I was wondering if the authors could explain the reason for deviations of the K-S metric for various n. I was expecting the K-S metric to decline by increasing n.