PUT 2019 Talk proposal: Evaluating Anonymity in Collaborative Systems

Killian Davitt

University College London
killian.davitt.17@ucl.ac.uk

This proposed talk concerns Anonymity in collaborative systems. The availability of anonymity in collaborative applications; Google Docs; slack etc is of increasing concern. Traditionally, Tor would be an obvious contender for introducing anonymity to platforms like these. Tors lack of resistance to global passive adversaries does mean however that we prefer the approach of using mixnet designs to introduce anonymity. The bulk of our discussion focuses on how we can evaluate the anonymity provided by modern mixnet designs, with a particular focus on the Loopix anonymity system.

The level of anonymity provided by mixnets and indeed all anonymity systems is usually evaluated by presenting the most effective attack that can be conducted under the system. Typically, attacks consider only simplistic scenarios where packets are sent independent of each other. A more realistic scenario, takes into account that packet streams are not independent; users reply to each other for example. When considering collaborative applications, we consider this to be of even greater importance. With $n > 2$ users collaborating, adversaries should operate with increased advantage, as the more users collaborate at once, the greater statistical dependence the packets have upon each other.

In an attempt to quantify this adversarial advantage, We detail our efforts to approximate a model of user behaviour using wikipedia article histories. In general, it is quite difficult to obtain data traces for collaborative behaviour. Simulating attacks against anonymity systems requires data to work upon and with no real data available we must look for a best approximation. Our theory, inspired by other work at PETs, is that the distribution of wikipedia article edits, is a reasonable approximation of user behaviour in collaborative systems (or at least, document editing collaboration). We detail our efforts so far, and how we hope to use the data in the future to provide better bounds on anonymity in mixnets.