De-anonymizing encrypted video streams

Prof. Dr. Ankit Singla, Systems @ ETH

Popular video streaming services on the Internet adapt the streaming video's quality continually in response to changes in network bandwidth. Further, each video itself can be encoded at each of these quality levels with a different number of bits, depending on its complexity – a simple two-dimensional cartoon can be shown to users in high quality with fewer bits than a dynamic sports video or rich action movie. Thus, video providers like Netflix encode each video separately, as shown on the left below, in a plot generated by Netflix researchers [1]. As the number of bits available (per second) increases, different videos show different improvements in quality. For instance, the line on the bottom of this plot corresponds to a complex video, for which large increases in bitrate are needed to ensure high-enough quality, while the steep line (top left) is for a simpler video, where high quality can be achieved with a small bitrate.

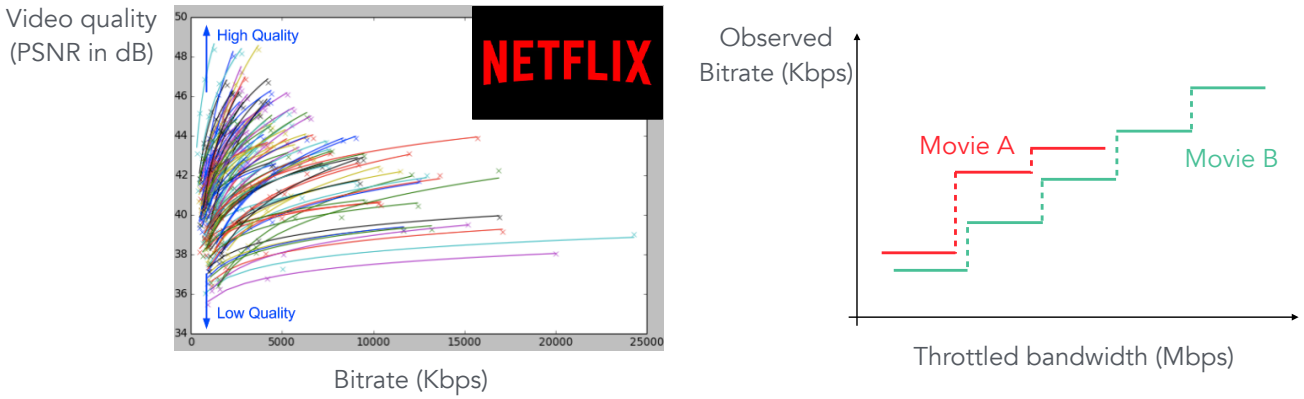

Figure 1: *Can we fingerprint encrypted videos based on their encoding optimization, and reveal what a user is watching?*

This way of optimizing video opens up an interesting question: can this optimization be used to de-anonymize encrypted video streams to reveal what a user is watching? If each video has a unique signature based on its encoding, corresponding to the above illustration, then perhaps by manipulating network bandwidth, an attacker can observe all the bitrates a video is streamed at, and thus identify the video (as shown on the right). The goal of this project is to explore the feasibility of such an attack, and if feasible, defenses against it. Note that this strategy could potentially be effective even against encrypted streams, and only depends on *average* observed traffic for a video stream over the network. Thus, if successful, it would expose a fundamental privacy problem with this way of optimizing video, and potentially require compromises to video streaming quality to preserve privacy.

The goal of this project is thus to build a system which can manipulate network bandwidth, observe video traffic, and reconstruct the "bitrate ladder" for a video being watched. We would then build a library of such bitrate ladders for a large number of videos, and then see how many ladders are unique, and how often videos can be successfully identified using an observed ladder. Time permitting, we will also explore the tradeoff between privacy and video quality: if the video service wants to obscure the bitrate ladders (*e.g.*, by not doing per-video encoding, but picking for each video one from a set of pre-decided ladders), how much worse is video performance?

[1] Per-Title Encode Optimization. Netflix: `https://goo.gl/JMCQNY`.

Contact Ankit Singla or Melissa Licciardello: {ankit.singla,melissa.licciardello}@inf.ethz.ch