Researchers discover clues for identifying Yik Yak users on college campuses

October 19 2016

Experiments by researchers at the NYU Tandon School of Engineering and NYU Shanghai have successfully cracked the veil of anonymity in Yik Yak, an ostensibly anonymous social media application.

Yik Yak thrives on anonymity. Whether it's praise for a local restaurant or, in a darker use of the application, a complaint or bullying comment about teachers or peers, Yik Yak users trust that their words are untraceable. Even Yik Yak's new policy requiring user pseudonyms preserves anonymity.Yik Yak is particularly popular on college campuses and has drawn criticism as a tool for harassment. The app has been downloaded more than a million times on Android mobile devices alone.

Keith Ross, the Leonard J. Shustek Distinguished Professor of Computer Science at NYU Tandon and Dean of Engineering and Computer Science at NYU Shanghai, will present the paper, You Can Yak but You Can't Hide: Localizing Anonymous Social Network Users, at the ACM (Association for Computing Machinery) Internet Measurements Conference in Santa Monica, California, this November.

Ross, his students, and colleagues from East China Normal University tested Yik Yak's susceptibility to localization attacks, reasoning that if it is possible to locate the geographical origin of a comment, or "yak," as it is commonly known, it may be possible to identify the person who posted it.

Experiments showed that yaks can, in fact, be localized through a fairly simple machine learning algorithm that an undergraduate computer science student could program and run in a matter of hours.

Ross and his collaborators localized yaks to within 300 feet and in one experiment identified the college dormitories from which yaks originated with 100 percent accuracy.

"The integrity of user anonymity is central to Yik Yak and similar anonymous social media apps, and this research shows that it's possible for a third party to compromise it," Ross said. "At this stage, we can narrow down a location to a building, which when combined with other side information could potentially de-anonymize the author of any given yak."

Ross and his team, which includes East China Normal University Professor Haifeng Qian and doctoral student Minhui Xue, and NYU Shanghai undergraduates Cameron Ballard, Kelvin Liu, Carson Nemelka, and Yanqiu Wu, conducted their experiments from Shanghai. They deployed Yik Yak on two U.S. college campuses using a common technique to trick the GPS in a smartphone into believing it was on those campuses. This was important because a yak appears only on smartphones in the vicinity of where the yak is sent.

The researchers designed an automated system to "place" themselves (through GPS coordinates) at many different locations in and around the campuses and record which yaks were available at each location. The system then used machine learning to process the recorded data to predict where each of the yaks was posted.

Ross explained that college students often post disparaging yaks about professors or fellow students. "It wouldn't be difficult for a professor to figure out the dorm from which a derogatory yak was posted, then

couple this information with student housing information to de-anonymize the yak, and that's concerning," he said.

The researchers note that their experiments used the same public information collected by other users of Yik Yak, and that they attempted to analyze only the location of messages generated by members of the research team. No outside participants were involved.

Ross and his colleague informed Yik Yak about the potential for localization attacks and recommended several potential privacy enhancements. Among them is improving localization authentication for users, which would make it easier to identify and block users employing forged GPS coordinates. Another strategy would be for Yik Yak to always display the exact same set of messages no matter where the app is being used on a campus.

Provided by NYU Tandon School of Engineering