Emily Evans
Final Report

As sharing options in online social networks (OSNs) continue to increase in complexity, users often upload content that is not only potentially sensitive for themselves but also for the other members of their social circles. This naturally leads to questions about group/multiparty access control. A user's comfort bears a lot of relevance in the study of access control, as users whose comfort levels may vary greatly have the potential to be beholden to another's access control decisions in a single party control model. This can lead to actual or perceived breaches of privacy, and exposure of sensitive content that may damage a user's reputation. Recently, researchers have constructed a game-theoretic model of group privacy decisions considering user comfort level and peer pressure [1]. The variable comfort is defined as a user's inherent comfort level with sharing content on OSNs. It does not include peer pressure, but is meant to reflect a user's inclination to share content online in the absence of both explicit and implicit peer pressure. Multiparty access control models seem to offer a potential solution to modelling sensitive content exposure. Studies of multiparty access control have successfully compared user study results to their models [1,2].

I worked with Dr. Anna Squicciarini over the summer of 2016 comparing her existing model to actual user choices on a fake OSN we constructed using Drupal. We began the summer by setting the goal of producing a user study by August. This would include adapting her existing model to use data generated from survey questions as input. Overall, my responsibilities included informal statistical analysis, constructing the initial survey, adapting the model, database management, and study design. Our research is yet to be published.

I will begin by describing the design of the study. Users were introduced to a fake OSN constructed using Drupal and asked to select privacy settings for a variety of images. First, users

filled out a survey about their online social networking habits. This survey included basic demographics (age, gender), and asked questions about how many "online" friends they had, which social networking platforms they use, and the privacy habits of both themselves and their close friends. Some of the Likert scale questions in the survey were a basis for the user's comfort score. Each of the questions used measured either comfort or discomfort. All comfort scores ϵ [0,1], 0 is no comfort, while 1 indicates maximum comfort. Each user's comfort was computed using the following formula.

$$\frac{\sum comfort\ questions}{\sum discomfort\ questions}$$

Dr. Squicciarini wanted an aesthetic that was more realistic than her previous studies' because she hypothesized that the participants' responses were not as accurate as they could be because the "fakeness" of the OSN was obvious to the average user. Therefore, they would be less likely to experience a realistic level of peer pressure because they were more aware that there would be no social consequences for their privacy decisions. With this in mind, we attempted to create a study that would encourage the participant to become personally invested in the process and the content which would yield more accurate results as the participants would be experiencing pressure more akin to that on an actual OSN. We decided to implement a friend-selection process instead of using the system she had previously utilized which involved introducing users to their existing friends after they completed the survey. Instead, we created twelve potential friend profiles from which users had to select five. After, the survey, users proceeded to a page that displayed each potential friend as an image and name. Users had to click on the profile, which contained more detailed information about the friend, in order to "become friends" with that profile. After they had selected five friends, they moved on to the actual study portion.

In this portion, users had to select images to upload, and choose privacy settings for the images. We constructed the image "upload" process in a way that we hoped would encourage users to have more personal stake in their content. Two Flickr albums were created; each had thirty images. One album was deemed "private" and contained images that depicted or suggested illegal activities and lewd behaviour. The other was deemed "public" and contained images of mundane and socially acceptable activities and objects. On each content page, the user was prompted to upload an image from one of the two albums. There were a total of twenty content pages. The first five used images from the public album, and the last fifteen used images from the private album. The user copied the URL of the image they wanted to upload into a text box, and then clicked "Upload". Then, we matched the URL to a URL stored in a table that also contained an arbitrary ID for each image and an "inherent" privacy level for each image. Private images had privacy levels of .25 or .5, while public images had privacy levels of .75 or 1.0.

The users were then shown their selected image. Underneath it, their friends' privacy settings for the image were displayed. The users then selected their own privacy setting from four possible choices: this image is visible only to me (.25), this image is visible only to select friends (.5), this image is visible to all my friends (.75), and this image is visible to everyone (1.0). Each privacy setting corresponds to a value between 0 and 1.

The last ten content pages used the model to predict and suggest privacy options. The user's comfort and "inherent" image privacy were used as input in the model that generated privacy setting predictions. I translated this model from Java to JavaScript and altered it to output only one setting. Five of the content pages presented all four possible settings, and the model-generated setting was saved alongside the rest of the data for analysis. On the other five pages,

the model-generated setting was displayed, and the user had to click “See more options” in order to select a different privacy setting.

References

[1] S. Rajtmajer, A. Squicciarini, C. Griffin, S. Karumanchi, and A. Tyagi. Constrained Social-Energy Minimization for Multi-Party Sharing in Online Social Networks. In Proceedings of the 2016 International Conference on Autonomous Agents and Multiagent Systems, pages 680-688, 2016.

[2] H. Hu, G.-J. Ahn, Z. Zhao, and D. Yang. Game theoretic analysis of multiparty access control in online social networks. In Proceedings of the 19th ACM Symposium on Access Control Models and Technologies, pages 93–102, 2014.