Presentation Speech

By Omar El-Sabrout and Joshua Fenech

Hello everybody,

One of the unquestionable things is that the Internet now has a major role in our lives on a daily basis. Such role has led to a lot of reactions by people and use the Internet as much as we can to get the best advantage of it. This requires personalizing internet services every day to our needs that differs from a person to another which leads to give service providers such as search engines information to accustom features to our needs. The story until now seems perfect but there is a twist. Our information that is sent to search engines are private and they are exploited to be used by advertisers to target ads towards our interests. It might not seem like a problem at first, but it indicates how our privacy needs to be defended. A lot of our data is stored by the service providers and it can be leaked due to their technical casualties or incompetence.

Until now, privacy on the internet is an important and unsolved issue and privacy preserving is not a point of interest for service providers because they want to know more about users. This motivated researchers to look for a technique that will empower the user to ensure the protection of his or her data or at least hide his or her interests from data mining techniques. Solutions so far focused on the side of the service providers to store encrypted or transformed data that can be still used for analysis. This has a major flaw, as it relies on the service providers to do this. The user has no chance of actively protecting his or her privacy. In this work, Wicker and Kramer suggest a new approach, empowering the user to take advantage of the same tool the other side has, namely data mining to produce data which obfuscates the user's profile. They apply this approach to search engine queries and use feedback of the search engines in terms of personalized advertisements in an algorithm similar to reinforcement learning to generate new queries potentially confusing the search engine. Overall, there are three main contributions of this paper:

• They introduce a new approach closely related to adversarial data mining (Lowd and Meek 2005) that utilizes data mining and machine learning as a method to defend a user's privacy.

• The new approach is explored in a common setting, i.e., the use of Internet search engines.

• A learning method is presented for environments where a user can get feedback from her or his counterpart.

The remainder of this paper is organized as follows: First, they give a brief discussion and define the user and search engine model. Next, they introduce the proposed method. Then, they give details of the experimental set-up and present experimental results.

Personalized advertisement is displayed depending on the submitted query by the user or the user's profile. Even if the user does not have a user account, the search engine builds a profile based on IP tracking and cookies to define the user's interests even if he or she was anonymous. Preprocessing the operation, ads are assigned to categories with cooperation with advertisers. Moreover, users are also assigned to categories based on their history and areas of interests.

In order for the privacy defense method to succeed, it needs a way or a standard to measure privacy and this is where the objective function presented in the paper comes in place. Explaining the objective function may take two minutes but it is pretty straight forward. This function weights the distance between the interest category and any other category by the estimated probability of the query belonging to that category. It sums over all such weighted distances in the tree. While this is the objective function, the authors aim to minimize, they are also interested in a low probability p j of A j belonging to the main user interest category κi in the below evaluation (with P being the vector of all probabilities p j for all categories κ j ∈ T. p can be estimated by any classifier. In this case, they used text mining-based classifiers fi for each category κi. The second component that is required for privacy defense is using the feedback of ads. This opens the discussion of category prediction of ads because search engines provide example queries for each category. These example queries or sample queries of category trees are the main input to train classifiers for ad categorization. Not only one classifier in this case, but as many classifiers as the number of available categories as every category has its own classifier. After certain training period, these classifiers can be used for more than classifying queries. Also, they can be used to classify any plain text which enables processing all text-based ads. As a result, prediction on ads works very well thanks to the similarities of structure between queries and text-based ads.

They also defined six possible actions that are used to select a category in relation to another category and the returned ads: Random, Same, Sibling, Most General, Most Specialized of Sibling, Distance-Based. Those actions are explained in details in the paper and presenting them would take a lot of time and kind of redundant. Considering the environment of the presented experiment in the paper, we find that it was redundant to execute the experiment with submitting queries from random categories as it does not provide relevant results and does not contribute in the significance of the privacy offense method. On the contrary, submitting queries from the category that is the furthest away from the user's interest category is more relevant to the privacy offense method. According to Wicker's experiment, all users submit random queries from their batch of interest categories in 10% of the cases. These outputs are based on using twenty categories in the experiment environment which we believe is sufficient in the context of an experiment. Upscaling the method would actually lead to more issues with greater number of users and interest categories. Despite that, it was fairly mentioned in the future work section that it is a major concern to continue working on the method and crucial to its development.

In conclusion, the experiment is successful to a certain extent with respect to the assumed limitations. Nevertheless, we still need further research and more elaborate experiment environments. There are more areas that deserve studying and should be tackled during the development of such tool like the fact that models of search engines also rely on time and date of the query which is a factor that should be considered and taken advantage of. At the end of the day, the major simplification of learning for only one interest is still the major concern and the greatest limitation of the tool. Future work is interesting as it can involve more feedback than just ads from search engines but also use more features that they provide to predict their models and reactions. This could lead to a more sophisticated tool and could provide a better privacy defense model.