Reaction to "Take This Personally: Pollution Attacks on Personalized Services"

1) Technical details (approach/technique) that you found novel/ Something specific you learned that you didn't know before

I have had a basic idea that the search result displayed by Google/Amazon/YouTube is somewhat related to your search history stored in either the browser or the account. However, this paper demos a quantitative relationship between the search history and the search result, which is novel to me.

2)Could I have done this work if I had the idea why or why not?

If I have the idea, I can do the work without any problem. The work didn't involve any private resource or technique. Actually one of my project proposal is to use the same method to pollute Google Ad Network in order to show the specified advertisement.

3)Is there anything I could do to repeat or validate?

I have repeated some work mentioned in this paper, such as repeatedly watch video B after watching video A to build connection between A and B, then validate that A is recommended for another new account that just finished watching B.

4) What is my best idea for follow on work that I could personally do?

I plan to verify whether similar strategies can be used to pollute advertisement networks such as Google Ads, whose result is believed also related to search / browse history.

5)What is my best idea for follow on work that I'd like to see the authors do?

One of the following work I want to see the authors do is to discuss more about the countermeasure to the pollution method mentioned in this paper. As the author mentioned that they shared their result with Google/Amazon/YouTube and get feedbacks, I am also interested in whether these companies have countermeasure to such an attack. The reason that I am interested in this is that I think it a little bit hard to distinguish normal browsing activities from XSRF attacks.

6)Any logistical experimental lessons I learned?

I don't think any aspect of logistical related lesson had been learnt from this paper.

7)How does this compare to the other papers we read? Most similar? How different? Other comparisons?

This paper is the first one we have read that talks about attacking related things, so I wouldn't say that it is similar to the previous papers we have read. However, many of the ideas that mentioned in this paper can be found related to some of the paper we have read before. One example is: the attack mentioned in this paper can also be conducted using commercial ad

networks.

8)What is your biggest criticism of the paper?

I think the biggest problem of this paper is that it didn't show a complete quantitative analysis to the security flaw it mentioned in this paper. One example is that when they conduct the research of creating relationship between one video and another, they didn't show the repeat time required for YouTube to think that this two movies are related. This problem almost happens to all the research result throughout this paper. I think if the author fix this problem, the result shown in the paper will be more accurate.