Reaction to "Trafficking Fraudulent Accounts"

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

This is basically an analysis of fraudulent accounts of Twitter, as well as the underground market supports related transactions. The idea is novel and interesting. However I don't think it contains any technical details that really is impressive.

One thing I really find interesting is the service of CAPCHA solver mentioned in the market.

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

I don't think we can do this work easily without the cooperation of Twitter. In the paper they mentioned that they got tons of valuable information from Twitter's database including registering IP, last login time and recent activity, which construct a significant part of their anti-fraudulent algorithm. Also, the cooperation with Twitter allows them to suspend suspect accounts then view for reactions, which is nearly impossible for independent thirdparty researchers.

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

The purchase of fraudulent accounts is basically open to everyone, which means we can duplicate their test of purchasing fraudulent accounts from underground market. The analysis of the Register name/screen name pattern also can be done without the help of twitter. However, without information we mentioned in the second question, I doubt the accuracy of such analysis.

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

One thing I am pretty interested in is the part that talking about how CAPCHA solving service affect the price as well as the accuracy for fraudulent account providers to register new account. As mentioned in the paper, a pure automatical CAPCHA solver has only less than 10% correctness. A research to CAPCHA solving techniques as well as the potential replacement for CAPCHA, such as graphic CAPCHA will be one thing I have interest in.

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

In the very last part of the paper the author mentioned that the fraudulent accounts providers are smart people. Only two weeks after the authors use their new way to block the fraudulent accounts, the providers have found workarounds to continue providing available accounts to potential buyers. I am very interested in how the authors will improve their classification algorithms so as to automatically detect and identify fraudulent accounts without the interference of human

6)Any logistical experimental lessons I learned?

Seems no related content in this paper

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

This is the first paper. So skip this part

8)What is your biggest criticism of the paper?

In the classification algorithm they used to identify fraudulent accounts, the authors try to find common substring from the screen name and account name. I didn't see detailed explanation about the reason that they choose to do this. However, I think there are very easy ways to avoid such kind of detection, liking maintains a big list of English/French or other Latin first/last names, and construct the user name in a human-like manner. If a name "Alice White" is chosen, then the user name can be "alicewhite2013" or something like that. If we count middle name in. There will be more possibilities. So it is easy to make there's no common patterns from the user name generated by one market provider. That's why I don't think it is a good idea to choose name as a classification factor.