Technical Disclosure Commons

December 2019

Ads that differentiate humans from bots

John Nicholas Dukellis

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Ads that differentiate humans from bots

ABSTRACT

Ad fraud, which occurs when automated software, e.g., bots, are utilized to activate advertisements is a major problem in the online advertising industry. This disclosure describes ads that request users to follow a sequence of instructions to detect if the user is a human or a bot.

KEYWORDS

- Ad fraud
- Click fraud
- Bot detection
- Automated agent
- Captcha
- Online advertising

BACKGROUND

Ad fraud, which occurs when automated software, e.g., bots, are utilized to activate advertisements is a major problem in the online advertising industry. If a bot is successful in activating an advertisement, e.g., by clicking on ad, the advertiser is charged for the ad being served while no benefit accrues to the advertiser. Thus, ad fraud reduces the effectiveness of online advertising which is problematic both for advertisers that want to use ad spends effectively and for advertising networks that want to provide reliable delivery of advertising for their customers.
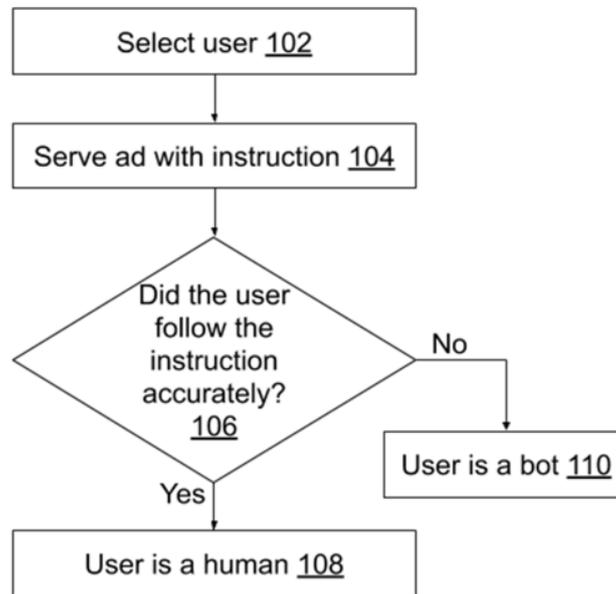
DESCRIPTION

Fig. 1: Ads that differentiate humans from bots

Fig. 1 illustrates online ads that can differentiate humans from bots. A user that activates an advertisement is selected (102) for verification, e.g., randomly or due to suspected ad fraud. An interactive ad that includes instructions is served to the user (104). The ad can be served, e.g., in HTML5 or another suitable format. The ad can include a reward such that the user receives a benefit such as commercial-free radio for thirty minutes upon completion of the ad experience within an app or website.

Instructions within the ad can be nested, e.g., the successful completion of a first instruction can result in the issuance of a second instruction and so on. Example instructions within the ad can be "click the button on the left," "click each button once," etc. A second-level instruction, issued upon the successful completion of a first instruction, can be, e.g., "click one more time, please."

Instructions can be provided in an image or via other modalities rather than in text to make it more difficult for bots to parse the instruction. Instructions can be timed, e.g., "click before 3 seconds," "click between 3 and 5 seconds," etc. For timed instructions, a timer is shown. The timing of ad presentation can be delayed to ensure that a bot isn't automatically clicking buttons immediately. Timed instructions can also be "don't press anything …," followed by a screen deactivation for a few seconds prior to the showing of the next instruction. To further increase the difficulty for bots that may be trying to read the results, instructions for wrong buttons are also loaded.

If the user follows the instructions accurately (106), then the user is determined to be a human (108). If the user does not follow the instructions accurately, then the user is determined to be a bot (110). The procedure can be repeated one or more times from start in order to rule out the possibility of error.
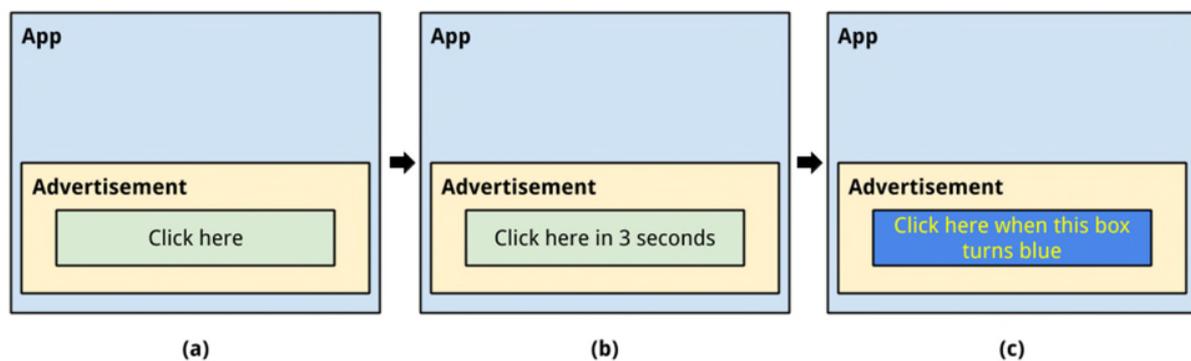

Fig. 2: Example ad that distinguishes bots and humans

Fig. 2 illustrates an example advertisement that distinguishes between bots and humans, delivered in an app. As shown in Fig. 2(a), the advertisement includes a first instruction "Click here." When a user successfully completes the task, a second task "Click here in 3 seconds" is shown, followed by a third task "Click here when this box turns blue." Successful completion of the three tasks confirms that the user is a human user, not a bot. The number, type, and sequence of tasks requested by the instructions can be

customized to prevent bots from completing the tasks. Advertisers and/or ad networks can choose verification mechanisms that are appropriate for the context, e.g., suitably complex to prevent bots, but easy enough that a human user can complete it without undue effort.

CONCLUSION

This disclosure describes ads that request users to follow a sequence of instructions to detect if the user is a human or a bot. The instructions can require users to perform specific actions that prove that the user is not a bot. The instructions can be served as a sequence, using different modalities, time delays, etc. to provide an adequate level of difficulty of automating performance of operations requested to be performed by the user. Users that complete successful verification can be provided a reward