Reducing Advertising Fraud by Verifying User’s Claimed Language and Locale

John Nicholas Dukellis
Reducing Advertising Fraud by Verifying User’s Claimed Language and Locale

ABSTRACT

In one scheme for defrauding online ad networks, a fraudster, typically outside the United States, operates large banks of mobile devices and perpetrates click fraud. To maximize payout, the fraudster devices pretend to be in the US or other high-income country, where the payouts are substantially higher. This disclosure describes techniques to detect such ad fraud by showing suspected fraudulent users an ad that involves a series of tasks whose solution requires working knowledge of the language of the locale the device is detected to be in. Languages other than that of the claimed device locale are made available. Selection of another language by the user increases the risk score of the device.

KEYWORDS

- Ad fraud
- Locale fraud
- Device language
- Device locale
- Click fraud
- CAPTCHA
- Risk score

BACKGROUND

In one scheme for defrauding online ad networks, a fraudster, typically outside the United States, operates large banks of mobile devices and perpetrates click fraud. To maximize payout, the fraudster devices pretend to be in the US or other high-income country, where the payouts are substantially higher. Although there are techniques available that attempt to detect if a device
is part of such a scheme, these techniques typically rely on signals, e.g., gyroscope settings, etc.,
whose availability may not persist or to which access is not always available.

DESCRIPTION

Fig. 1: Reducing advertising fraud by verifying the user’s claimed language and locale

Fig. 1 illustrates reducing advertising fraud by verifying the user’s claimed language and
locale, per the techniques of this disclosure. Devices suspected to be part of an ads-fraud scheme
are shown an ad that involves a series of tasks (102). Solution of the tasks requires working
knowledge of the language of the locale the device is pretending to be in. Delays are introduced
between tasks to reduce the fraudulent user’s throughput.

For example, tasks can be created to have the appearance of parts of a research series
rather than suspicion of fraud. For example, “is there a cat in this image” can be a sample
question. If the tasks are consistently performed incorrectly (104), the risk score of the device as
a potentially fraudulent device is increased (106). In addition to the language of the locale the device is pretending to be in, other languages are made available for the user to select. The selection of another language (106) by the user, e.g., if the user selects “switch to Malay” or “switch to Spanish,” such selection is an indication that the device is not physically in the locale it is detected to be in. In such a case, the risk score of the device is increased. If the tasks are performed consistently well in the language of the claimed device locale, the device is considered to not be part of the advertising fraud scheme.

CONCLUSION

In one scheme for defrauding online ad networks, a fraudster, typically outside the United States, operates large banks of mobile devices and perpetrates click fraud. To maximize payout, the fraudster devices pretend to be in the US or other high-income country, where the payouts are substantially higher. This disclosure describes techniques to detect such ad fraud by showing suspected fraudulent users an ad that involves a series of tasks whose solution requires working knowledge of the language of the locale the device is detected to be in. Languages other than that of the claimed device locale are made available. Selection of another language by the user increases the risk score of the device.