Private Zone: Secure Group-Based Advertising for Online Social Networks

Sanaz Taheri Boshrooyeh, Alptekin Küpçü and Öznur Özkasap
Department of Computer Engineering, Koç University, İstanbul, Turkey
{staheri14,akupcu,oozkasap}@ku.edu.tr

ABSTRACT

Services provided as free by Online Social Networks (OSN) come with the cost of privacy concerns due to the closure of users personal information to the untrusted providers. To protect user privacy, existing solutions utilize data encryption. While data encryption protects the data confidentiality against unauthorized entities including server, it prevents the server in performing advertising hence monetizing users' data. Addressing these problems, we propose Private Zone system that provides privacy preserving group-based advertising for OSNs. Private Zone protects users' privacy in an efficient manner, and it is formally proven to be secure against honest but curious non-colluding servers.

KEYWORDS

Advertising, Online Social Networks, OSN, Security, Privacy

1 PROBLEM DEFINITION AND MOTIVATION

Advertising in OSNs is a vital functionality as it serves as a financial resource for the network providers. Users security concerns about sharing the personal and private information with untrusted and curious servers lead researchers to design secure OSNs. However, such designs fall short in providing privacy preserving advertising functionality satisfying users' privacy requests. Existing solutions do not suit the secure OSN designs. They enforce the user and advertiser (either or both) to stay in contact with the server (stay online) so that the server can match user's profile with the advertising request in a private manner [3]. This not only poses a huge computation overhead on the user/advertiser but also degrades the performance of the system as the server's working time depends on the user's online time. Other solutions do not address data confidentiality [2] (of user or advertiser) while it is the key concern in any secure OSN. Addressing the incompatibility of existing works with the objectives of secure OSNs, we propose Private Zone which is a privacy preserving advertising system for secure OSNs, and any secure OSN can incorporate Private Zone into its design.

2 PRIVATE ZONE SYSTEM

Private Zone system overview is depicted in Fig.1. The server named S_{OSN} collects user and advertiser data and carries out the main computation overhead of the system, whereas the other server named S_{match} helps S_{OSN} to find the advertisers target audience. Servers are non-colluding. Users share their encrypted profiles, consisting of user's interests (e.g. football, art, music), with S_{OSN}. Advertisers willing to promote their products submit their encrypted advertising request, consisting of a collection of attributes of target users, to S_{OSN}. One of the two servers could be the OSN provider, while the other server could be a governmental organization or a privacy service provider that assists OSN provider to protect users privacy.

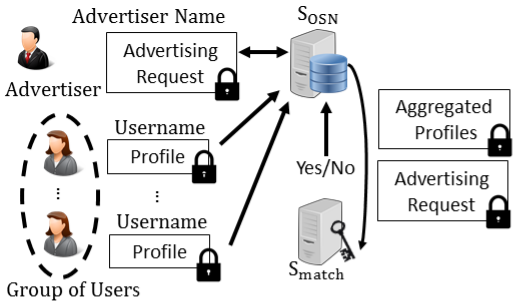

Figure 1: Private Zone system overview

As a solution to the security breaches imposed by the personalized advertising, we propose the notion of group advertising. In the personalized advertising, if the server matching the profile and advertising request collude with either party, it gets the content of the non-colluding party's data based on the matching result. Whereas, in group matching, each advertising request is checked against a group of profiles. If the number of matched profiles exceeds a threshold (given by the advertiser) the group is marked as the target and the advertisement is presented to all the members. In this design, the number of target users per group may leak whereas for the sake of privacy the target users' identities remain unknown. We define user's privacy as the unlinkability of user's attributes and the user name.

In Private Zone design, user profile and advertising requests are modeled by bloom filters which are data structures for set representation and membership checking. Users are divided into groups of equal size based on their arrival times. In order to manage users into separate groups and prevent the S_{OSN} making groups of users arbitrarily (as it violates the user's privacy), Private Zone benefits from zero-sum secret sharing which ties profiles of each group together. The remedy is to aggregate profiles of group members. We propose a novel invertible aggregation algorithm where the S_{OSN} performs aggregation on the encrypted profiles and S_{match} can extract individual profiles from the aggregated value [1]. S_{match} performs the matching procedure and responds to S_{OSN} accordingly (Yes/No). In order to perform aggregation on the encrypted profiles, we utilize an additive homomorphic encryption. In the poster presentation, we plan to provide Private Zone design details, algorithms and its security proof.

REFERENCES

[1] Sanaz Taheri Boshrooyeh, Alptekin Küpçü, and Öznur Özkasap. 2017. Private Zone: Secure Group-Based Advertising for Online Social Networks (under submission).
[2] Saikat Guha, Bin Cheng, and Paul Francis. 2011. Privad: practical privacy in online advertising. In *NSDI*.
[3] Florian Kerschbaum. 2012. Outsourced private set intersection using homomorphic encryption. In *CCS*. ACM.