PRISM: PRIVACY-AWARE INTEREST SHARING AND MATCHING IN MOBILE SOCIAL NETWORKS

OBJECTIVE:

The objective of this system is to profile matchmaking of mobile social networks.

ABSTRACT:

In a profile matchmaking application of mobile social networks, users need to reveal their interests to each other in order to find the common interests. A malicious user may harm a user by knowing his personal information. Therefore, mutual interests need to be found in a privacy preserving manner. Here, we propose an efficient privacy protection and interests sharing protocol referred to as Privacy-aware Interest Sharing and Matching (PRISM). PRISM enables users to discover mutual interests without revealing their interests. Unlike existing approaches, PRISM does not require revealing the interests to a trusted server. The inherent mechanism reveals any cheating attempt by a malicious user. PRISM also proposes the procedure to eliminate Sybil attacks. We analyze the security of PRISM against both passive and active attacks. Through implementation, we also present a detailed analysis of the performance of PRISM and compare it with existing approaches. The results show the effectiveness of PRISM without any significant performance degradation.

INTRODUCTION:

In this paper, we present a protocol named as PRISM (PRivacy-aware Interest Sharing and Matching) that securely matches the private information of two users. Our objective is to improve the existing matchmaking protocols and help mobile users to securely perform

matchmaking without revealing unnecessary information. The main contributions of our paper are as follows:

- ✓ PRISM provides a secure and privacy preserving mechanism in order to find mutual interests of users.
- ✓ The paper discusses unaddressed attacks on user privacy and provides effective means to prevent these attacks. These include attacks during the interests matching and interest revealing phases.
- ✓ We suggest a mechanism that aims to provide protection against Sybil attacks by limiting a user to at most one device.
- ✓ Unlike existing approaches, the trust assumptions on trusted third party (TTP) are significantly reduced by not revealing user interests to the TTP.
- ✓ The implementation of PRISM and subsequent comparison with existing approaches show that PRISM provides better protection against various attacks without any significant degradation in performance.

EXISTING SYSTEM

In previous protocols, it is possible to create many identities using any social network site. Although these sites attempt to restrict a user to have a single identity associated by some unique credentials such as an email or phone number, but in real life it is very hard to detect a violation. We suggest the idea of restricting a user to have at most one identity on a device. We argue that a Sybil attack with as many devices as number of identities is very hard to prevent. A realistic approach can be to restrict a user to use only one identity on single device.