Master project in Information Security at the University of Luxembourg

Title: Anonymizing Social Graphs Against Active Attacks

The Security and Trust of Software Systems group, led by Prof. Dr. Sjouke Mauw, is looking for outstanding master students who want to develop their master thesis within our group.

Project description

A novel privacy measure, named (k, ℓ)-anonymity, has been recently introduced in [2] to prevent active attacks in social networks. Active attacks were proposed in 2007 by Backstrom et al. [1], based on the creation and insertion in the network of *attacker nodes* controlled by the adversary. The attacker nodes could be either new accounts with pseudonymous or spoofed identities (Sybil nodes), or legitimate users in the network who collude with the adversary. Attacker nodes establish links with other nodes in the network (also between them self) aiming at creating a sort of fingerprint in the network. Once the social graph is released, the adversary just need to retrieve such a fingerprint (the attacker nodes) and use it as a hub to re-identify other nodes in the network. Backstrom et. al. proved that $O(\sqrt{\log n})$ attacker nodes in the network can compromise the privacy of arbitrary targeted nodes with high probability, which makes active attack particularly dangerous.

In September 2015, the master student Bochuan Xuan at the University of Luxembourg empirically showed that graph satisfying $(k, 1)$-anonymity for some $k > 1$ indeed protect user's privacy. The drawback, however, is that (k, ℓ)-anonymity imposes a strong structural requirement on the graph, which is hard to achieve without a huge information loss.

General goal. In this project we will propose modifications to the (k, ℓ)-anonymity concept. Such modifications are aimed at relaxing the structural requirement imposed by (k, ℓ)-anonymity on social graphs. To do so, we will consider different types of adversaries in social networks. We will also perform experiments on real-life social graphs in order to show that graphs satisfying the proposed theoretical privacy measure also satisfy privacy against well-known active attacks.

Contact Information

For further inquiries please contact:

- Prof. Dr. Sjouke Mauw (`sjouke.mauw@uni.lu`) or
- Dr. Rolando Trujillo (`rolando.trujillo@uni.lu`)

References

[1] Lars Backstrom, Cynthia Dwork, and Jon Kleinberg. Wherefore art thou r3579x?: Anonymized social networks, hidden patterns, and structural steganography. In *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, pages 181–190, New York, NY, USA, 2007. ACM.

[2] Rolando Trujillo-Rasua and Ismael G. Yero. k-metric antidimension: a privacy measure for social graphs. *Information Sciences*, 328:403 – 417, 2015.