Safebook: Privacy Preserving Online Social Network

L. Antonio Cutillo, R. Molva, M. Önen

Online Social Network (OSN) applications and services such as picture sharing, wall posting, and the like, nowadays have a strong impact on the way users interact with each other. Catering for a broad range of users of all ages, and a vast difference in social, educational, and national background, these applications and services allow even users with limited technical skills to share a wide range of personal information with a theoretically unlimited number of partners. This advantage comes at the cost of increased security and privacy exposures for users for two main reasons: first of all, users tend to disclose private personal information with little guard, and secondly, existing OSN applications severely suffer from vulnerabilities in their privacy protection or the lack thereof. The exploitation of these vulnerabilities[1] can lead a malicious user to launch many different types of attacks such as Id theft, profile cloning or secondary data collection[2]. Furthermore, even assuming a perfect protection from such malicious users, legitimate users are still exposed to a major orthogonal privacy threat, since in all existing OSN applications, the service provider has access to all the data including some private information stored and managed by the application itself and can misuse such information easily.

Since the access to users' private data is the underpinning of a promising business model[1], current OSN services are not likely to address this problem in the near future. Researchers recently proposed to design the OSN application based on a peer-to-peer architecture in order to avoid centralized control over users' data. While in one hand a peer-to-peer model seems to be a good candidate to build a privacy preserving solution that avoids centralized control, on the other hand it lacks any a priori trust relationships among parties. Among existing peer-to-peer based solutions, Safebook[3] leverages the social trust that is available as part of the very application in order to build a network of trusted peers that store OSN users' data.

In Safebook each user's data is partitioned and replicated and the encrypted replicas of a user's data are stored at the nodes of that user's trusted friends. The untraceability of the communications during look-up and data retrieval operations is assured thanks to an additional feature of Safebook in that the messages between a requester node and a friend's node that serves the request always route through several hops in order to hide a user's social links that are reflected by the OSN graph. Safebook defines two identities for each peer, namely the node and user identifiers, to prevent the disclosure of sensitive friendship information originating from an analysis on the data flows. Moreover, Safebook also prevents Sybil attacks thanks to the presence of a Trusted Identification Service which is contacted only once during the user

[1] http://techcrunch.com/2008/06/23/modeling-the-real-market-value-of-social-networks/

registration phase in order to generate a unique and unforgeable identifier per user. The introduction of this third party does not impact the decentralized nature of Safebook's architecture since it is not involved in any data communication or data management operation.

Even though Safebook is one of the few peer-to-peer OSN projects to enjoy from a complete architecture and a prototype implementation[2] there has not been so far any comprehensive investigation about the fundamental performance and security questions that can be raised by peer-to-peer OSN architectures in general. An initial performance study on Safebook first establishes the relationship between privacy and the residual lifetime of a multi-hop communication link deriving an analytical model of data availability in terms of privacy and on-line probability of nodes in the OSN. The main parameters of the data partitioning and replication scheme are determined based on the same data availability model. The feasibility of Safebook is further assessed using real-life data such as social graphs from several universities and nodes' on-line times from Skype. Apart from confirming Safebook's feasibility in large scale networks with affordable data availability rates and sufficient privacy, this study additionally shows a very strong trade-off between performance and privacy such that delay and data reachability are inversely proportional to privacy and the characteristics of social networks also have a strong impact on both performance and privacy. The results of this study are valid for any peer-to-peer based online social network applications.

References

[1] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. *All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks*. WWW 2009, Madrid.

[2] L. A. Cutillo, M. Manulis, T. Strufe. *Security and Privacy in Online Social Networks.* Chapter book of "Handbook of Social Network, Technologies and Applications", Springer, October 2010, ISBN: 978-1-4419-7141-8

[3] L. A. Cutillo, R. Molva, T. Strufe. *Safebook : a privacy preserving online social network leveraging on real-life trust*. "IEEE Communications Magazine", Vol 47, N°12, Consumer Communications and Networking Series, December 2009 , pp 94-101

[2] http://www.safebook.us/prototype.html