Security and Privacy in Online Social Networks

Mots clés :

- Directeur de thèse : refik MOLVA
- Co-encadrant(s) :
- Unité de recherche : Laboratoire de recherche d'EURECOM
- Ecole doctorale : Ecole Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal: Divers

Résumé du projet de recherche (Langue 1)

Social network applications allow people to establish links and exchange information based on various interests such as professional activities, hobbies, et similia. Several commercial social networking platforms that came to light recently suddenly became extremely popular at the international arena. Apart from obvious advantages in terms of fast community building, rapid exchange of information at the professional and private level, social network platforms raise several issues concerning the privacy and security of their users. The goal of this thesis is to identify privacy and security problems raised by the social networks and to come up with the design of radically new architectures for the social network platform. As current social network platforms are based on centralized architectures that inherently threat user privacy due to potential monitoring and interception of private user information, the goal is to design social network platforms based on a distributed architecture in order to assure user privacy. New mechanisms are investigated in order to solve some classical security and trust management problems akin to distributed systems by taking advantage of the information stored in the social network platforms. Such problems range from trust establishment in self-organizing systems to key management without infrastructure to cooperation enforcement in peer-to-peer systems. This thesis suggests a new approach to tackle these security and privacy problems with a special emphasis on the privacy of users with respect to the application provider in addition to defense against intruders or malicious users. In order to ensure users’ privacy in the face of potential privacy violations by the provider, the suggested approach adopts a decentralized architecture relying on cooperation among a number of independent parties that are also the users of the online social network application. The second strong point of the suggested approach is to capitalize on the trust relationships that are part of social networks in real life in order to cope with the problem of building trusted and privacy-preserving mechanisms as part of the online application. The combination of these design principles is Safebook, a decentralized and privacy-preserving online social network application. Based on the two design principles, decentralization and exploiting real-life trust, various mechanisms for privacy and security are integrated into Safebook in order to provide data storage and data management functions that preserve users' privacy, data integrity, and availability. Apart from the design of Safebook, a significant part of the thesis is devoted to its analysis and evaluation using various methods such as experimenting with real social network platforms. Finally, this thesis presents an implementation of Safebook that is written in python and can be executed on multiple operating systems such as Windows, Linux and MacOs. The Safebook implementation is a multithread event-driven application composed by different managers in charge of building and keeping the social network and P2P overlays, performing cryptography operations and providing the main social network facilities such as friendship lookup, wall posting and picture sharing through a user interface implemented under the form of a webpage. The Safebook client is licensed under GPLv3 and can be downloaded from the Safebook website at the link http://www.safebook.eu.