Chapter 16
On the Use of Formal Methods to Enforce Privacy-Aware Social Networking

Néstor Cataño Collazos
The University of Madeira, Portugal

Sorren Christopher Hanvey
The University of Madeira, Portugal

Camilo Rueda Calderón
Pontificiad Universidad Javeriana, Colombia

ABSTRACT

This chapter discusses the use of formal techniques and formal verification tools to ensure privacy-aware social networking; hence users of social-networking sites can predict what the consequences of updating their privacy settings are. A formal methods approach is presented for modeling and comparing social-network privacy policies, and for checking whether a user's privacy policy can coexist with other policies within a social networking site. The authors present the Poporo tool implementing the approach. Poporo builds on a predicate calculus definition for social networking written in B that models social network content, people in the network, friendship relations, and privacy policies that are modeled as permissions to access content. Several examples of privacy-awareness social networking are also shown using Poporo.

INTRODUCTION

In recent years, on-line social network services in the form of web-sites such as Facebook, MySpace, LinkedIn and Hi5 have become popular tools that allow users to publish content, share common interests and keep up with their friends, family and business connections. A typical social network user profile features personal information (e.g. gender, birthday, family situation), a continuous stream of activity logged from actions taken on the site (such as messages sent, status updated, games played) and media content (e.g. personal photos and videos). The web offers numerous

DOI: 10.4018/978-1-4666-8111-8.ch016

services that suit users' needs based on information extracted from personal profiles. The privacy of this information has become a significant concern. Users may upload media they wish to share with specific friends, but do not wish to be widely distributed to their network as a whole. Some examples of privacy issues are, users can gain access to a photo album of an unknown user simply because a friend is tagged in one of the images or because the user has no control over what an application used by another user with access to one's content can share. Back-doors also exist to facilitate casual connections such as allowing an unknown user to gain access to profile information simply by replying to a message he or she has sent.

Furthermore, social networking sites have conflicting goals. Although respecting the privacy of their client base is important, they must also grow and expand the connections between their users in order to be successful. This is achieved by allowing users to connect over common interests by exposing content through less restrictive policies. Social-networking policies are constantly changed to grant users more control over who can access user's content. This constant change leaves users in the dark on what actually their policies entail, which is exacerbated by the fact that users find stipulating detailed privacy settings to be challenging (Bonneau, Anderson, & Church 2009). Additionally, it is not always possible to trust the social networking site to uphold users' policies as became evident from Facebook privacy breaches in 2009 (Pepitone, 2011) when Facebook changed its privacy policies without informing its users, resulting in content from private groups being made public. Such a breach called for a mechanism for independently checking compliance of new policies to existing policies.

However, privacy means something different to everyone. Based on the diverse types of privacy rights and violations, it is evident that technology has a dual role in privacy: new technologies give rise to new threats to privacy rights, at the same time, new technologies can help preserve privacy. Formal methods can address privacy issues, but privacy raises new challenges, and thus new research opportunities, for the formal methods community (Tschantz & Wing, 2009).

With the explosion of the Internet, privacy is finally getting serious attention by the scientific community. More and more personal information about us is available online. For example with cloud computing and social networks, we further entrust third parties with the storage and management of private information in places unknown to us. We are making it easier for others to find out about our personal habits, tastes, and history.

Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data about one's self. Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. In some cases these concerns refer to how data is collected, stored, and associated. In other cases the issue is who is given access to information. This includes whether an individual has any ownership rights to data about them, and/or the right to view, verify, and challenge that information.

In the context of social networking sites (SNS) from a user's perspective, privacy is enforced through a privacy policy, which is a statement that discloses some or all of the ways a system gathers, uses, discloses and manages the user's data. Personal information can be anything that can be used to identify an individual, not limited to but including; name, address, date of birth, marital status, contact information or any content shared by a user within a SNS. From the perspective of the SNS system, it is a statement that declares a policy on how it collects, stores, and releases personal information. It informs the user what specific information is collected, and whether it is kept confidential or shared with partners and if so, how.