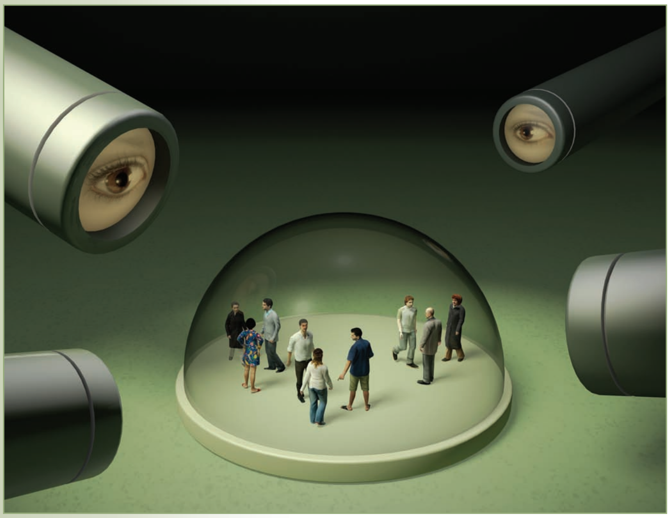

Security and Privacy in Social Networks

Gail-Joon Ahn
Arizona State University

Mohamed Shehab
University of North Carolina at Charlotte

Anna Squicciarini
Pennsylvania State University

The Internet's wide adoption has contributed to online social networking sites' thriving popularity, which is evident in the attention such sites receive from both the media and academia. Over the past several years, several social networking sites have arisen to facilitate social interactions on the Internet while revolutionizing how online users interact with their friends, coworkers, colleagues, family, and even strangers. Moreover, some social networks let users further partition their sets of friends based on social community, organization, geographical location, or how well they know each other.

Most social networking sites offer the basic features of online interaction, communication, and interest sharing, letting individuals create online profiles that other users can view. One of the most important issues we must immediately address in this context is the security and privacy of sensitive information, which is generally any data an adversary could use to cause significant harm to users. Such data might include financial information, which an attacker could use to perpetrate identity theft, or medical information, such as health conditions, diagnoses, or treatment histories. Unfortunately, current trends in social networks indirectly require users to become system and policy administrators to protect their online contents. Further complicating this issue is social networks' rapid growth as well as their continual adoption of new services.

A New Paradigm

The use of personal information in social networks raises new privacy concerns and requires insights into security problems. Online social networks have recently emerged as a challenging research area with a vast reach and application space. Several studies and recent news reports have highlighted the increased risk to personal data processed by online social networking applications, as well as the user population's lack of awareness. In general, the privacy issue in social networking is coupled with the identifiability and linkability of the information available in this social setting, its possible recipients, and its potential uses. Protecting information's identifiability

1089-7801/11/$26.00 © 2011 IEEE

and linkability is quite challenging given that even those sites that don't disclose users' personal information might provide enough data to identify and link a profile's owner. Possible recipients for such personally identifiable information include hosting servers for the social networking sites, the network itself, and third parties that might abuse or misuse such critical and sensitive information.

In addition, a new paradigm for security involves the need to address issues of interpersonal relationships and flexibility in online social networks. For instance, a user could share his or her personal photo album with family members but not with colleagues from work. Social network sites enable users to create a limited profile and select which other users map to it. Such primitive security mechanisms have only limited expressiveness for controlling user-to-user interactions, especially in a dynamic social network. The need for new security mechanisms based on metrics such as risk, trust, and social metrics is becoming more compelling.

Social networks' security and privacy requirements still aren't well understood or fully defined. Nevertheless, it's clear that they'll be quite different from classic security and privacy requirements because social networks involve user-centric concerns and allow multiple users to specify security policies on shared data. So, we must bring a depth of security experience from multiple security domains and technologies to this field, as well as a breadth of knowledge about social networks.

In this Issue

This special issue aims to encompass research advances in security and privacy in social networks and share corresponding state-of-the art technologies for realizing such advances. We've carefully chosen four articles that deal with novel technologies and methodologies for securely building and managing social networks and relevant secure applications, as well as cross-cutting issues.

The first article, "Modeling Unintended Personal-Information Leakage from Multiple Online Social Networks," by Danesh Irani, Steve Webb, Calton Pu, and Kang Li, describes an information-leakage measure for quantifying how much information is available about a user. The authors seek a way to protect users' privacy and reduce information leakage in the social Web. They emphasize the importance of effective countermeasures for personal information leakage.

In "Location-Related Privacy in Geo-Social Networks," Carmen Ruiz Vicente, Dario Freni, Claudio Bettini, and Christian S. Jensen introduce geo-social networks (GeoSNs), which extend social networks by providing context-aware services focused on associating location with users and content. The authors investigate four privacy aspects related to location, absence, co-location, and identity privacy in GeoSNs, addressing potential attacks and protection techniques.

"Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam," by Markus Huber, Martin Mulazzani, Gerhard Kitzler, Sigrun Goluch, and Edgar Weippl, examines friend-in-the-middle attacks on social networks that might impersonate social network applications and demonstrates how adversaries can use such critical attacks to automatically harvest social data. This article helps determine the vulnerability of all major social networks and highlights how primitive current protection strategies are.

Finally, "Preserving Relation Privacy in Online Social Network Data," by Na Li, Nan Zhang, and Sajal K. Das, addresses issues and challenges with regard to the disclosure and protection of relation privacy over online social network data. The authors classify existing techniques for protecting relation privacy based on the potential exposure of user identities.

Although the methods in this special issue are a good start, the need still exists to both advance existing privacy theories for social networks and improve technologies for sharing personal information. Rather than simply blocking access and limiting users' exposure, we strongly believe that we must provide new ways for users to share content with others, without requiring them to be connected via conventional social relationships. Also, we must enable users to track the actions of other selected users with whom they share a social relationship, but whose actions with regard to some content aren't completely trusted. These features will eventually let users distinguish real and digital social relations and act accordingly when sharing data in social networks.

Acknowledgments

We would like to express our gratitude and appreciation to those who substantially contributed to this special issue: editor-in-chief Michael Rabinovich and associate editor-in-chief Maarten van Steen, for their cheerful and vigorous cooperation, the reviewers for their helpful and invaluable comments that enhanced the quality of the selected articles, and the authors for contributing outstanding articles and providing revised versions in a timely manner.

Gail-Joon Ahn is an associate professor at Arizona State University. His research interests include information and systems security, vulnerability and risk management, access and identity management, and security architecture for distributed systems. Ahn has a PhD in information technology from George Mason University. He serves as an associate editor for *ACM Transactions on Information and System Security* and an associate editor-in-chief for *IEEE Transactions on Dependable and Secure Computing*, and is a senior member of both IEEE and the ACM. Contact him at gahn@asu.edu.

Mohamed Shehab is assistant professor at the University of North Carolina, Charlotte. His research interests include distributed access control, secure distributed collaboration in multidomain environments, Web services security, and security for social networks. Shehab has a PhD in computer engineering from Purdue University. Contact him at mshehab@uncc.edu.

Anna Squicciarini is an assistant professor at the Pennsylvania State University. Her research interests include trust negotiation techniques for peer-to-peer systems, digital identity management techniques for federated systems, privacy enhanced technologies, and access control and privacy for social networks and Web 2.0 platforms. Squicciarini has a PhD in computer science from the University of Milan. Contact her at asquicciarini@ist.psu.edu.

cn *Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.*

IEEE Intelligent Systems provides peer-reviewed, cutting-edge articles on the theory and applications of systems that perceive, reason, learn, and act intelligently.