Privacy Protection for Social Networking

Alice BODEA
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
bodea.alice21@gmail.com

Abstract

Social networking APIs integrate third-party content into the site and give third-party developers access to user data. These open interfaces enable popular site enhancements but pose serious privacy risks by exposing user data to third-party developers. We address the privacy risks associated with social networking APIs by presenting a privacy-by-proxy design for a privacy-preserving API that is motivated by an analysis of the data needs and uses of Facebook applications. Nearly all applications could maintain their functionality using a limited interface that only provides access to an anonymized social graph and placeholders for user data. Since the platform host can control the third-party applications' output, privacy-by-proxy can be accomplished without major changes to the platform architecture or applications by using new tags and data transformations.

Keywords: social networking, privacy, security

References

[1]. R. Gross and A. Acquisiti. Information relevation and privacy in online social networks. In Workshop on Privacy in the Electronic Society, 2005.
[2]. L. Sweeney. Uniqueness of Simple Demographics in the U.S. Population. Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA, 2000.
[3]. M. Helft and B. Stone. Myspace joins Google alliance to counter Facebook. The New York Times, 2 November 2007.
[4]. www.privacyrights.org/
[5]. C. Abram. Thirty million on Facebook. The Facebook Blog, 10 July 2007.
[6]. T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer. Social phishing. Communications of the ACM, 50, 2006.