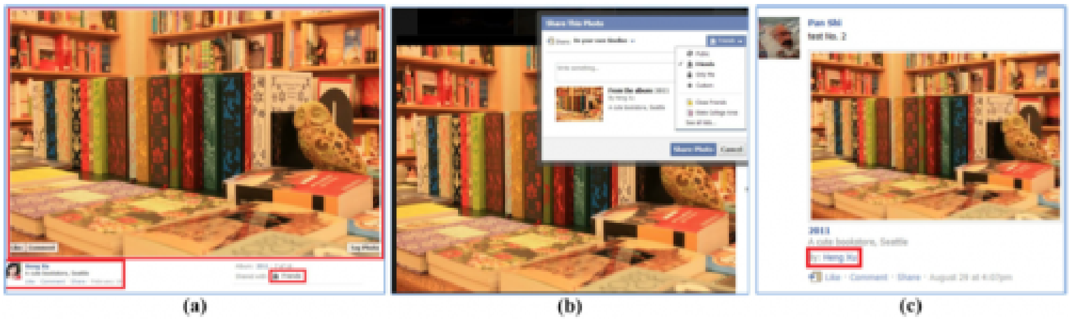
PHYS ORG

Researchers aim to safeguard privacy on social networks

March 31 2015



Potential privacy breach on Facebook: (a) information owner shares a photo to friends; (b) a friend re-shares the photo to public; (c) the photo is displayed on the friend's wall, open to public, without consent from owner. Credit: University of Kansas

At the end of 2014, Facebook reported 1.39 billion monthly active users. In the meantime, 500 million tweets were sent each day on Twitter. Indeed, social networks have come to dominate aspects of our lives. But all our social sharing comes with a price. Last year, the Pew Research Center found 81 percent of Americans feel "not very" or "not at all secure" using social media sites when they want to share private information with another trusted person or organization.

Now, a researcher at the University of Kansas' Information and Telecommunication Technology Center is investigating solutions that could shore up personal privacy on leading social media sites.

"Part of the problem is the business model," said Bo Luo, associate professor of electrical engineering and computer science. "Social network providers aggressively expand their user bases and promote socialization and sharing. They're not really motivated to protect user privacy until the privacy concern becomes significant enough to impact the growth of their business."

Now, with a pair of three-year grants from the National Science Foundation amounting to about $500,000, Luo and Dongwon Lee of Pennsylvania State University, are developing technology to shore up user privacy.

The project will hone methods to detect the discrepancies between users' information-sharing expectations and actual disclosure; design a user-centered yet computationally efficient formal model of user privacy in social networks; and develop a mechanism to effectively enforce privacy policies in the proposed model, according to the researchers.

Luo said many users of social networks remain unaware that shared information isn't necessarily kept to their intended group of contacts and that parties with malicious intent easily may gain access. Researchers call this privacy problem a "leaky boundary."

"Large amounts of personal information are voluntarily posted to social networks," he said. "Often, the true audience of such information is much larger than the data owner perceives. That is, when 'Alice' posts a message to a social network, it's intended for selected users—for example, she thinks, 'I want my friends to see this'—however, many more users, including adversaries, may have access to the message."

Thus, seemingly trivial sharing on social networks could leave users open to "undesired information disclosures" and "information aggregation attacks."

"Each single message only contains a very small amount of information," Luo said. "However, by aggregating all the posts from a certain user, the adversary learns a lot about this user."

Luo sees a prevalent contradiction—privacy concerns voiced by users who are at the same time playing fast and loose with their own data—as a call to action.

"Studies have shown a massive disconnection between users' privacy perceptions and their behaviors—widely known as the 'privacy paradox,'" Luo said. "That is, most users do not take appropriate actions to protect their information, although they express concerns on the privacy of such information."

To help with the problem, the researchers plan to design a formal privacy model that will restrict information sharing to users' social circles.

"Social circles of a user's network are hidden structures of closely connected clusters," Luo said. "For instance, a user's high-school friends may constitute a circle, while his or her colleagues belong to a different circle, and his or her family members constitute yet another circle."

Luo and his team will develop a real-time privacy enforcement tool that would provide privacy protection across several sites and detect leaky boundaries that allow private information to travel beyond social circles.

Lastly, the researchers will carry out user studies to shrink the gap between perceived and actual privacy on social media and improve decision making in sharing personal information.

Until then, Lou suggested that users of sites like Facebook, Twitter and Google+ choose the strictest privacy protections available on those sites, even though "many of the existing privacy protection mechanisms are somehow difficult to use."

"Users should always employ privacy protection functions provided by social network providers," he said. "Users should also be conservative and think more about the possible consequences before they post any potentially sensitive information."

Provided by University of Kansas

Citation: Researchers aim to safeguard privacy on social networks (2015, March 31) retrieved 18 April 2024 from https://phys.org/news/2015-03-aim-safeguard-privacy-social-networks.html