Software improves p2p privacy by hiding in the crowd

April 8 2009

Researchers at the McCormick School of Engineering and Applied Science at Northwestern University have identified a new "guilt-by-association" threat to privacy in peer-to-peer (P2P) systems that would enable an eavesdropper to accurately classify groups of users with similar download behavior. To thwart this threat, they have released publicly available, open source software that restores privacy by masking a user's real download activity in such a manner as to disrupt classification.

P2P systems are incredibly popular, enabling new and important Internet applications such as voice over IP (VoIP) and file sharing. These systems work by establishing network connections between machines that cooperate to perform a common goal. While many researchers have pointed out that the data exchanged over these connections can reveal personal information about users, an interdisciplinary collaboration between Fabián Bustamante, associate professor of electrical engineering and computer science, Luis Amaral, associate professor of chemical and biological engineering, and Roger Guimerà, research assistant professor of chemical and biological engineering, shows that only the patterns of connections — not the data itself — is sufficient to create a powerful threat to user privacy.

The team of researchers, which includes graduate students David Choffnes (electrical engineering and computer science) and Dean Malmgren (chemical and biological engineering), and postdoctoral fellow Jordi Duch (chemical and biological engineering), studied connection patterns in the BitTorrent file-sharing network — one of the largest and most popular P2P systems today. They found that over the course of weeks, groups of users formed communities where each member consistently connected with other community members more than with users outside the community.

"This was particularly surprising because BitTorrent is designed to establish connections at random, so there is no *a priori* reason for such strong communities to exist," Bustamante says. After identifying this community behavior, the researchers showed that an eavesdropper could classify users into specific communities using a relatively small number of observation points. Indeed, a savvy attacker can correctly extract communities more than 85 percent of the time by observing only 0.01 percent of the total users. Worse yet, this information could be used to launch a "guilt-by-association" attack, where an attacker need only determine the downloading behavior of one user in the community to convincingly argue that all users in the communities are doing the same.

Given the impact of this threat, the researchers developed a technique that prevents accurate classification by intelligently hiding user-intended downloading behavior in a cloud of random downloading. They showed that this approach causes an eavesdropper's classification to be wrong the majority of the time, providing users with grounds to claim "plausible deniability" if accused.

The research team implemented this strategy in software that has already been made available as a seamless extension to the popular Vuze BitTorrent client. The software, named SwarmScreen, downloads randomly-selected content in a way that prevents eavesdroppers from distinguishing it from user-desired content. SwarmScreen allows users to control the impact of these connections on the download performance for the data they want to keep.

More information: SwarmScreen is available for download on the Aqualab website or via the Vuze plugin installation menu. For more details about this work, visit aqualab.cs.northwestern.edu/pr … cts/SwarmScreen.html

Source: Northwestern University (news : web)

Citation: Software improves p2p privacy by hiding in the crowd (2009, April 8) retrieved 24 April 2024 from https://phys.org/news/2009-04-software-p2p-privacy-crowd.html