Facebook privacy flaw nailed at Lugano workshop

March 22 2012, by Nancy Owano

(PhysOrg.com) -- As if Facebook has not has enough invasion-of-privacy problems, a pair of researchers have come up with one more reason why Facebook cannot rest. Shah Mahmood and Yvo Desmedt, Chair of Information Communication Technology at University College London, want the wide world of Facebook-account users to know that there is a hole in Facebook's settings that allows stalkers, whether they are personal mischief makers or governments, to spy on accounts without the account holder aware that anything is wrong. The technique is called “cloaking” and it works when the attacker deactivates and reactivates accounts, which Facebook allows.

Deactivation is temporary in Facebook; the attacker can reactivate his or her account and keep repeating the on-off switch any number of times. There is no set limit. The victim is not notified of the switch.

The two researchers have revealed Facebook’s privacy loophole in which the attacker temporarily deactivates his or her account to avoid detection and removal from the friend list, but reactivates to spy on the victim’s data. Mahmood and Desmedt's test used a Facebook account under a pseudonym. They asked people to friend them and then they deactivated their account, reactivated for short periods of time, checked their friends' content, and deactivated again. This is what the researchers mean by "cloaking," checking on “friends” regularly by reactivating for ten-minute periods only, and crawling over hundreds of profiles and tracking activities.

The researchers note in their findings how easy it was for them to add over 4300 users and maintain access to their Facebook profile information. "We tested the cloaking attack for 261 days and none of our Facebook friends unfriended during the course."

The loophole appears to be a dream for wanting to nail broader profiles as well, as the security weakness enables attackers to monitor both the individual victim and his or her links. That way, the spies could learn about relationships, political and otherwise, dates the people became Facebook friends, and events they attended. As the authors note, Facebook now has the feature of browsing friendships and this would help the attacker in analyzing the bond between two victims by browsing their friendship which provides information including the month and year when they became Facebook friends, mutual friends, and photos.

As easy as it is to “cloak,” the researchers say the problem can be fixed in a number of ways and they offer several solutions for the loophole. For example, Facebook might move to flag users who activate and deactivate their accounts in a suspicious way, over and over, and these individuals might be monitored. With enough reason, Facebook could even move to ban them from Facebook.

Another suggestion is that users be notified about activation and deactivation actions of "friends." They could report any suspicious activity back to Facebook.

The Facebook loophole study was presented at the IEEE International Workshop on Security and Social Networking (SESOC 2012) in Lugano, Switzerland on March 19.

More information: Shah Mahmood, Yvo Desmedt: Your Facebook Deactivated Friend or a Cloaked Spy (Extended Abstract), arXiv:1203.4043v1 [cs.SI] arxiv.org/abs/1203.4043

Abstract
With over 750 million active users, Facebook is the most famous social networking website. One particular aspect of Facebook widely discussed in the news and heavily researched in academic circles is the privacy of its users. In this paper we introduce a zero day privacy loophole in Facebook. We call this the deactivated friend attack. The concept of the attack is very similar to cloaking in Star Trek while its seriousness could be estimated from the fact that once the attacker is a friend of the victim, it is highly probable the attacker has indefinite access to the victims private information in a cloaked way. We demonstrate the impact of the attack by showing the ease of gaining trust of Facebook users and being befriended online. With targeted friend requests we were able to add over 4300 users and maintain access to their Facebook profile information for at least 261 days. No user was able to unfriend us during this time due to cloaking and short de-cloaking sessions. The short de-cloaking sessions were enough to get updates about the victims. We also provide several solutions for the loophole, which range from mitigation to a permanent solution

Citation: Facebook privacy flaw nailed at Lugano workshop (2012, March 22) retrieved 27 April 2024 from https://phys.org/news/2012-03-facebook-privacy-flaw-lugano-workshop.html