

Technical Perspective

Fake ‘Likes’ and Targeting Collusion Networks

By Geoffrey M. Voelker

THE FOLLOWING SCENARIO might sound like fiction. You and a million of your closest Facebook friends are going to band together to artificially improve your social networking reputation. You will willingly give a reputation manipulation service such as “official-liker.net” authorized access to your Facebook account. The manipulation service will cleverly exploit an authentication vulnerability in third-party Facebook apps to automate actions with your account. To use the service, you will view ads or pay explicit fees. The service will then use your account to “like” another Facebook account under their control—and that account will “like” yours back. You and others gain fake “likes,” presumably improving your perceived online social standing, and the reputation service makes a profit.

But this scenario, and the problem it presents to Facebook and other successful online social networks, is both a very real and challenging problem: How to completely undermine this abusive activity without negatively impacting your users (who are knowingly and entirely complicit in the abuse) or changing how apps authenticate (because that would add friction to the app ecosystem).

The following paper presents a rigorous study that explores this reputation manipulation ecosystem, ultimately working with Facebook to examine ways to stop this kind of large-scale online social networking abuse. The manipulation services are called collusion networks since the users who knowingly participate collude with each other to generate fake actions. In their work, the authors describe how to use honeypot accounts to infiltrate the collusion networks and reveal how they operate. The authors detail how the collusion networks take advantage of an authentication vulnerability using leaked access tokens to perform their ac-


tions, and comprehensively measure the extent and activity of the collusion networks they find. Who would do this? Over a million Facebook users. How many apps are vulnerable? More than half of the top 100 third-party Facebook apps. How many services are exploring this unexpected business opportunity? More than 20 such services. Finally, can these collusion networks be safely and effectively shut down? Yes.

As a final effort, the authors performed a series of careful interventions with Facebook against these services. Consider the defensive perspective of the online social network. Companies know which accounts are using collusion networks, which apps are being exploited to perform collusion, and who the collusion networks are. But services cannot shutdown the user accounts: the users are legiti-

The following paper presents a rigorous study that explores the reputation manipulation ecosystem, ultimately working with Facebook to examine ways to stop this kind of large-scale online social networking abuse.

mate, and services want them to continue to use the platform. They also cannot shutdown the apps, or how apps perform authentication: the apps have millions of legitimate users, and ease of app development relies upon the client-side token-based authentication.

The authors’ most important contribution is showing how companies can target collusion network activity and, crucially, how collusion networks respond to such interventions. The authors first experimented with a range of rate limit strategies. For access tokens used by the collusion networks, Facebook limited the rate of actions generated by accounts using such access tokens in a variety of ways, from throttling actions per day to invalidating all new tokens identified each day. Impressively, the collusion networks were able to successfully react to all token rate limit strategies, finding ways to adapt to the interventions and maintain their abusive activity. The authors then used network-based identifies, such as the IP addresses of the machines generating Facebook likes or, more broadly, the autonomous systems from which collusion activity originated. Using network identifies was much more effective, undermining nearly all collusion network activity. One of the key lasting contributions of this work is the careful, detailed methodology of experimenting with interventions and evaluating how the collusion networks respond and adapt.

Reputation has value and manipulating reputation can be a profitable enterprise. Read on for a fascinating study exploring this phenomenon in Facebook’s online social network. 

Geoffrey M. Voelker (voelker@cs.ucsd.edu) is a professor in the Department of Computer Science and Engineering at the University of California San Diego, CA, USA.

Copyright held by author.