Dagstuhl Seminar 17372

Cybersafety in Modern Online Social Networks

September 10 - 13, 2017, Schloss Dagstuhl, Wadern, Germany

Organizers:
Jeremy Blackburn (Telefónica Research – Barcelona, ES)
Emiliano De Cristofaro (University College London, GB)
Michael Sirivianos (Cyprus University of Technology – Lemesos, CY)
Thorsten Strufe (TU Dresden, DE)

The range of malicious activities perpetrated on online social networks is regrettably wide, ranging from malware and spam to controlling fake and compromised accounts, to artificially manipulating the reputation of accounts and pages, spreading false information and terrorist propaganda. Unfortunately, research in this field has looked at these problems in isolation, almost exclusively relying on algorithms aimed at detecting malicious accounts that act similarly. This ultimately yields a catandmouse game, whereby providers attempt to make it more and more costly for fraudsters to evade detection.

This prompts the need for a multifaceted, multidisciplinary, holistic approach to advancing the state of knowledge on cybersafety in online social networks, and the ways in which it can be researched and protected. In this field, there exists a number of interconnected, complex issues that cannot be addressed in isolation, but have to be tackled and countered together. This Dagstuhl Seminar, we identify and plan to focus on the most relevant issues in cybersafety, as well as to explore both current and emerging solutions. Specifically, we identify four problems that are the most pressing both in terms of negative impact and potential danger on individuals and society, as well as challenging open research problems calling for a multidisciplinary approach:

1. Cyberbullying and Hate Speech
2. Cyber Fraud and Scams
3. Reputation Manipulation and Fake Activities
4. Propaganda and Radicalization

The main goal of this seminar is to bring together researchers working on all aspects of cybersafety, including security, privacy, human factors, economics, sociology, law, and psychology. We aim to discuss many facets of the problem, both technical and nontechnical, and jointly identify measures to advance the state of the art and identify promising research avenues.
Examples of issues to be debated include:

- How do we define cyberbullying and online harassment in a way that captures their inherent ambiguities and subjectiveness?
- How do perpetrators of these activities exploit technological tools to increase their effectiveness? How do cyberbullies and online harassers organize and choose targets?
- What are the different types of cyber fraud activities and how might we cluster different types of scams, based on psychological, sociological, situational and technical variables so as to better design countermeasures?
- What data are ethically and socially acceptable to draw upon in detection and prevention of cyber fraud?
- What variables are important in enabling us to distinguish those who have become single or repeat victims from nonvictims?
- What are the current mitigation schemes adopted by social networks to counter reputation manipulation and their limitations?
- What are the economics and legal mechanisms governing fake activities?
- What can be done to make it economically unviable for fraudsters to engage in reputation manipulation and fake activities?
- How does online radicalization happen?
- Are there specific demographics that are more susceptible to being radicalized? How is online radicalization different from other types of online abuse?

Authors: Jeremy Blackburn, Emiliano De Cristofaro, Michael Sirivianos, and Thorsten Strufe