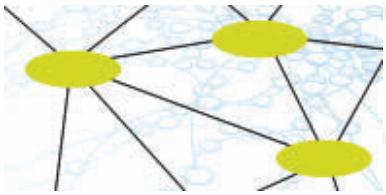
only hope that future designers of socialbots with different goals will adhere to Asimov's Three Laws of Robotics [7] to reduce the risk of harm to the human systems in which they operate.

@tinypirate is a government drone in New Zealand who spends his spare time concocting schemes and convincing smarter friends to act on them. @AeroFade is a computer security researcher from New Zealand with an Hons. in computer science, interested in studying how online culture shapes the offline world.



The Socialbot Network: Are Social Botnets Possible?

Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu

Online social networking services (SNSs) have far exceeded their original goal of connecting friends, family, and acquaintances. Today third parties use SNSs as an effective medium to reach out to millions of active users via social media campaigns. The effectiveness of such campaigns and the long-term survival of SNSs rely on the trust among these users, which is materialized through publicly exposed social connections (e.g., friendships on Facebook, follower/followee relationships on Twitter).

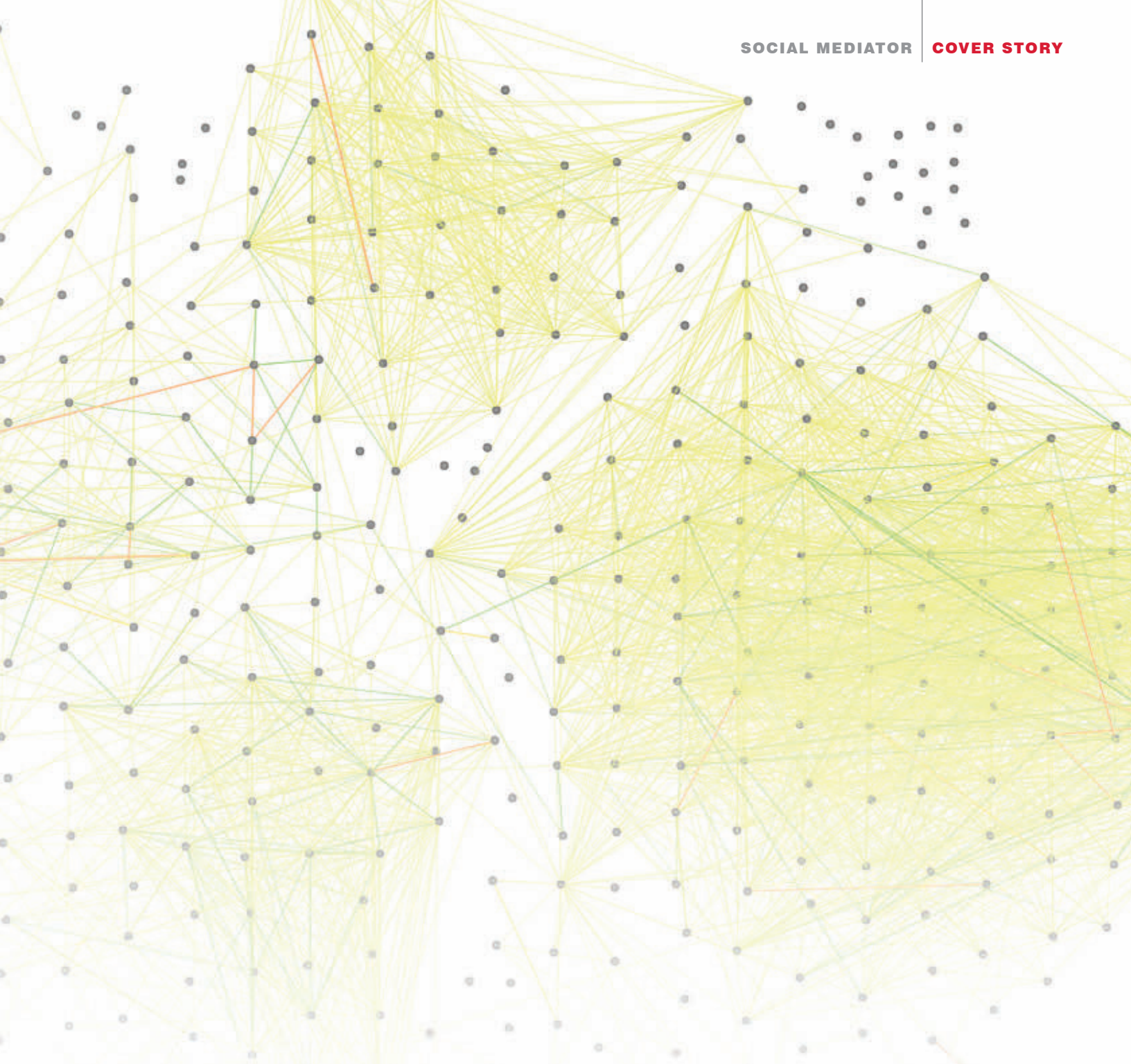
A new attack vector on such networks thus becomes possible: A malicious entity that not only controls a large number of SNS profiles but also establishes an arbitrarily large number of connections with human users can threaten the long-term health of the SNS ecosystem.

To counter this threat, today's SNS security defenses block hijacked SNS accounts that are usually controlled by spam bots. Such defenses flag accounts as malicious based on their behavioral patterns. However, the robustness of these defenses against socialbots—automated profiles designed to mimic human behavior—is relatively unexplored.

To fill this gap, we adapted the design of existing botnets and built a socialbot network (SbN), a group of programmable socialbots that are controlled by an attacker using a software controller called the botmaster [8]. We deployed our SbN prototype, consisting of 102 socialbots and a single botmaster, on Facebook for eight weeks during the spring of 2011. We selected Facebook as the target SNS for two reasons: It is the largest SNS today, and it represents a friendship network where users connect mostly with friends and family but not with strangers. Overall, the socialbots sent 8,570 connection requests, out of which 3,055 were accepted.

Our experiments yielded multiple findings. First, we demonstrated that SNSs are vulnerable to large-scale infiltration. Not only is it feasible to automate the operation of an SbN with minimal resources, but users' behavior in SNSs can also be exploited to increase the likelihood of a successful infiltration. For example, we observed that the more friends a user has, the less selective she will be when screening out friendship requests sent by a socialbot. Moreover, users are even less selective when they have mutual friends with socialbots, when the chance of accepting a friendship request from a bot reaches up to 80 percent. Second, and equally important, bots that mimic real users (e.g., by posting intriguing status updates crawled from the Web) make it difficult for other users and SNS security defenses to identify them as bots.

One implication of a successful infiltration is that private information is exposed. Our experiments showed that large volumes of private data (e.g., birth dates, postal and email addresses, phone numbers) that are publicly inaccessible could



be harvested by socialbots. More important, large-scale infiltration can lead to erosion of trust between users, which is the basic fabric of the SNS ecosystem.

As with any other socio-technical system, countermeasures require both technical and human factors. From the technical side, SNSs can make the SbN operation more difficult and less profitable by, for example, improving the accuracy and the speed of detecting and blocking the bots. From the user side, increasing awareness and helping users make better decisions when they receive connection requests are also avenues for further research.

Yazan Boshmaf (http://ece.ubc.ca/~boshmaf) is a Ph.D. student at UBC interested in social network security and adversarial learning. Ildar Muslukhov (http://ece.ubc.ca/~ildarm) is an M.Sc. student at UBC interested in online social networks and mobile security. Konstantin (Kosta) Beznosov is an associate professor at UBC doing research in computer security. Matei Ripeanu leads the Networked System Laboratory (http://netsyslab.ece.ubc.ca) at UBC and is interested in large-scale distributed systems with a focus on self-organization and decentralized control.

Socialbots and Marketing

DuBose Cole

Within the realm of marketing, the use of social robotics currently has limited exposure. Initially, their use may seem at odds with digital marketing for brands, especially in social media, as the most productive activity comes from a genuine conversation with the consumer. However, socialbots are still a