Unique Security Challenges for Online Social Networks
ICT-FORWARD 2009 Invited Talk

Joseph Bonneau, University of Cambridge Computer Laboratory

May 4, 2009

Once a niche application for students, social networking sites have recently exploded in mainstream popularity. The largest have become complex systems with hundreds of millions of users, billions of photos, and thousands of third-party applications. The oft-derided buzzword 'Web 2.0' has become prophetic as SNSs repeat the growing pains of the larger Internet. SNS operators have re-implemented existing protocols such as email, instant messaging, RSS, and OpenID within their own walls. They have implemented their own markup languages and spawned an industry of third-pary software developers.

Not surprisingly, SNSs are continually criticised for their perceived insecurity. The list of threats is well-known: phishing, spam, cross-site scripting, malware, data and identity theft. This talk, however, will focus on what is different and argue that many of these problems are fundamentally more challenging in the SNS environment.

- **Easy Social Engineering**–The existence of easy access to the social graph makes many scams more effective. Phishing emails are orders of magnitude more effective from friends than from strangers. 419 scams have also become common, where a compromised account is used to request an emergency wire transfer from a "friend."

- **Personal Data**–Privacy concerns are intensified by the highly personal nature of uploaded information. Encouraged by SNS operators, younger users view their profile as a private space and upload highly sensitive data. Because social networks require sharing to be useful, it has proved difficult to design usable access controls. There are also many gray areas for content produced collaboratively.

- **Data Centralisation**– Network effects predict that a natural monopoly should arise for general-purpose SNSs, and indications are that Facebook is becoming dominant. The centralised architecture of SNSs places all user data in operator-controlled siloes. This data is attractive to many third parties because it is easy to access, complete, and consistently formatted. It also contains much information that is not available elsewhere, in particular the social graph. SNS operators have retained broad legal rights to use this data however they see fit.

- **Economics**– The business model for SNS operators remains undefined. Most proposed revenue streams involve compromising user privacy to some extent. There are also serious questions about liability for privacy violations between the SNS operator and third-party developers.