

# Trust and Privacy Exploitation in Online Social Networks

**Kaze Wong**, *Macao Polytechnic Institute*

**Angus Wong**, *The Open University of Hong Kong*

**Alan Yeung and Wei Fan**, *City University of Hong Kong*

**Su-Kit Tang**, *Macao Polytechnic Institute*

**This survey presents the pitfalls of security protection in online social networks and identifies common attack methods. A harmless proof-of-concept malware app demonstrates the vulnerability of online social networks and the significance of the user's mentality.**

Online social networks let users keep in touch with families, friends, and colleagues in an easy and convenient way, but they also present various security risks. Large-sale online social networks have become very popular owing to advances in network and mobile technologies.<sup>1,2</sup> Their popularity has, in turn, drawn the attention of attackers and intruders, who want to exploit this large population to spread malware or steal personal information. Some online social networks, such as Facebook, LinkedIn, and Google+, require users' real identity. Online social networks also preserve a great amount of users' confidential and financial information, including credit card information.

There are two major types of attacks in online social networks. The first is accomplished by exploiting security loopholes in the networks, and the second is accomplished by abusing trust among users. The second type can sometimes be easier to accomplish, because humans aren't always cautious. We focus here on this type of attack, discussing the pitfalls of the security in social networks and popular attack methods that exploit the user's trust. We also present a proof-of-concept Facebook app to demonstrate the risks in social networks.

## Security Pitfalls in Social Networks

Online social networks involve many services, stakeholders, user behaviors, and business

considerations, resulting in a complicated security paradigm with the following pitfalls.

### **Confusing and Complicated Settings**

Social network companies are looking for ways to make money. They're introducing new products and services, such as video advertising, multimedia streaming, and automated photo tagging, and are trying to expand payment services. They're also attempting to debut mobile tools and apps to exploit the fast-growing mobile market.

Such endeavors might make the social network look more versatile and state of the art, but they might also complicate the network and make it more difficult to ensure there's a unified strategy for controlling privacy and security.

### **Convenience over Security**

Enforcing security measures can result in higher operational costs and lower performance, but social network providers are likely even more concerned with any inconveniences the security measures cause in terms of users sharing content or developers distributing apps. Such inconveniences can hinder attempts to obtain a bigger market share.

Consequently, the default privacy settings in social networks are commonly set to a level favorable for sharing (and thus less secure).

### **Friends' Influence on Privacy Control**

Your data's security also depends on the security settings of the friends with whom you share content. For example, even if you have a high security setting, if you share your content with friends, and one of your friends is hacked, your data will be exposed to the attacker. Thus, the strength of your security level is as weak as that of your friend with the lowest level of security.

### **Inferred Information**

Even if you don't disclose your information, it can be inferred by analyzing your and your friends' shared content. For example, suppose that you haven't entered any personal information in your profile. However, if your friends tell Facebook that they are from college ABC, and in many of your group photos, you're with those people at the college, then you're probably from the same college. Ensuring privacy in social

## **Related Work in *IT Pro***

- K.W. Miller and J. Voas, "Who Owns What? The Social Media Quagmire," *IT Professional*, vol. 14, no. 6, 2012, pp. 4–5; doi: 10.1109/MITP.2012.116.
- M. Chau et al., "A Blog Mining Framework," *IT Professional*, vol. 11, no. 1, 2009, pp. 36–41; doi: 10.1109/MITP.2009.1.
- J.R. Michener, "Defending Against User-Level Information Exfiltration," *IT Professional*, vol. 14, no. 6, 2012, pp. 30–36; doi: 10.1109/MITP.2011.112.
- A.K. Jain and D. Shanbhag, "Addressing Security and Privacy Risks in Mobile Applications," *IT Professional*, vol. 14, no. 5, 2012, pp. 28–33; doi: 10.1109/MITP.2012.72.
- R. Jain and D. Sonnen, "Social Life Networks," *IT Professional*, vol. 13, no. 5, 2011, pp. 8–11; doi: 10.1109/MITP.2011.86

networks can sometimes require more than just a technical solution.

### **New Incentives for Attackers**

User data is essential for many business opportunities, which presents incentives for various

**The strength of your security level is as weak as that of your friend with the lowest level of security.**

attacking or intrusion activities. The data—user profiles, posted text messages, shared pictures, or "like" actions—can be harnessed to help advertisers better market their products.

Various apps and people thus use different approaches to try to collect as much data from you as possible. One way to achieve this legitimately is to have your permission. In fact, an app that looks like an interesting game might be designed with the primary purpose of collecting your data. When installing such an app, you might have given the "game" permission (intentionally or unintentionally) to access your profile, albums, and friends list.

### **Common Attack Methods**

Here, we introduce possible attack methods for online social networks, which we used in our proof-of-concept Facebook app.

## Malware

Malware is malicious software that appears in the form of codes/scripts or other kinds of software. Hackers can use it to collect sensitive user information. Hackers can spread malware in online social networks by sharing malicious URLs that direct users to third-party websites, where the users are asked to download a (malware) file. If a user downloads and executes the file, he or she will become infected and will in turn send the same malicious URLs to his or her friends. For example, a malware named “Ice IX” has stolen credit card information from many Facebook users.<sup>3</sup>

## Spam, Scams, and Phishing

Because of the trust relationship among users of online social networks, these networks are effective places for advertising, phishing, and scamming in the form of spam. Social spam can cause traffic overload, result in a loss of trust,<sup>4</sup> as well

**Social spam can cause traffic overload, result in a loss of trust, as well as consume system bandwidth and compromise user patience.**

as consume system bandwidth and compromise user patience.<sup>5</sup> Besides advertising, phishing can also take advantage of the privacy leakage in online social networks. More than 70 percent of the spam on Facebook advertises phishing websites.<sup>6</sup>

## Botnet

A botnet is formed by compromising a number of computers on the Internet. Attackers can control botnets by sending messages through online social networks.<sup>7</sup> Elias Athanasopoulos and his colleagues performed an experiment to turn Facebook into a botnet.<sup>8</sup> They developed an application that would export HTTP requests to a victim host. In an estimate of their botnet’s firepower, they claimed that if an attacker deployed a malicious app with millions of users, the victim host would have to serve hundreds of Gbytes of unwanted data per day.

## Identity Forgery

Identity forgery happens when an attacker accesses someone’s private information and uses it to pretend to be that person. It occurs not only in real world but also in online social networks.<sup>9</sup>

## Excess Permissions

People can access online social networks using smartphone apps. Before installation, these apps ask users for certain permissions, such as access to contacts or photos stored on the phone, although some permissions aren’t actually necessary for the provided function.

Another form of excess permission is requested by third-party apps on online social networks. For example, people can use third-party apps on Facebook to play games or share photos and videos. Some apps request access to the personal data of the user’s friends or request permission to post messages on user’s behalf. This can be dangerous if the apps use the data in unlawful ways, and it can lead to privacy leakage.

## Our Proof-of-Concept Facebook App

In our experiment, we first created a proof-of-concept Facebook app, which is a harmless malware. Our app is a social game bonus collector, which automatically collects game bonuses shared by friends of the user. By default, after installation, a Facebook app can access a user’s name, gender, networks, and friend list. Our app requests three extended permissions from the user:

- *email*—permission to obtain the user’s email address;
- *read\_stream*—permission to read all posts (status updates, pictures, or links) in the user’s newsfeed; and
- *publish\_actions*—permission to, on the user’s behalf, publish posts on the user’s wall, comment on others’ posts, and “like” posts published by others.

(See <http://developers.facebook.com/docs/reference/login/extended-permissions> for more information.)

The app seemingly has two main functions: analyze the newsfeed and present a tutorial. By reading the user’s newsfeed, the app can filter game bonus posts and extract the links to claim the bonuses au-

tomatically. After claiming the game bonuses, the app posts to the user's wall to advertise the app to others. A video tutorial, which redirects users to a video-sharing website, teaches people how to use the app.

However, in reality, the app is implicitly performing additional tasks. It accesses the user's friend list to construct a social graph and analyze the various relationships. It also reads the user's newsfeed to analyze not only the user's posts but also his or her friends' activities. Finally, the "watch tutorial" function redirects users to a bogus website that looks similar to a well-known corporate website, where users are asked to upgrade a browser plug-in before watching the video. The download link then points to a malicious file.

Figure 1 shows the system architecture of our proof-of-concept program, in which we're acting as an attacker. The server is fully controlled by us (the attacker). The Web server (www.ni-hacking.com) is used to host a fake website that can do phishing and spread malware. The application server is used to host our Facebook app program, which we refer to as the *Facebook app engine*.

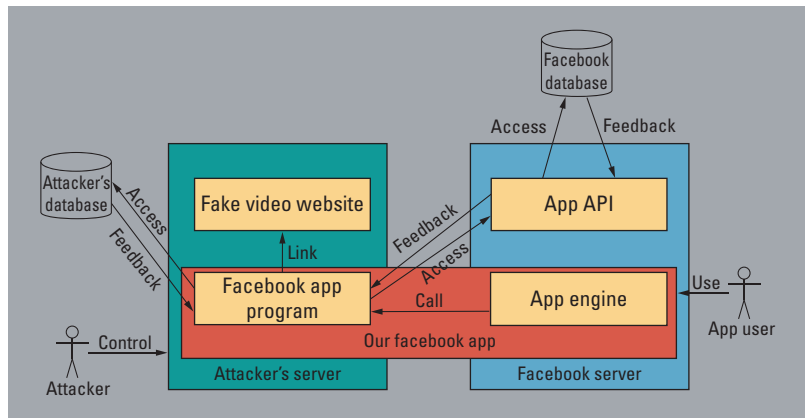
## Operations

Here, we outline the operations of our proof-of-concept experiment.

First, we post a link to the app on our Facebook walls, recommending the app to our friends (see Figure 2a). When our friends see it and click on the link, the installation process starts. During the process, some access permissions are requested (see Figure 2b).

In our app, users can choose the "analyze newsfeed" function, as shown in Figure 2c. The function will be provided to users, but meanwhile, our app can secretly read all posts from the users and stores them in our (attacker) server for data analysis.

Or, if users choose the "watch tutorials" function, they're redirected to a fake YouTube site, where they're asked to upgrade a browser plug-in to watch the video tutorials (see Figure 2d). When the users click on the download link, the system links to a malicious malware. (In our system, we just link to the download page of Adobe Flash so that users aren't actually attacked.)



**Figure 1. System diagram of our proof-of-concept experiment. The diagram includes malware, phishing, botnet, identity forgery, and excess permissions activities.**

In our proof-of-concept Facebook app, the five attacking methods discussed earlier were or could be used. The malicious app, with excess permissions granted by users, can

- obtain users' email address so attackers can spam them,
- post to users' wall on their behalf so the app can attract other users, and
- read all posts in users' newsfeed for information analysis.

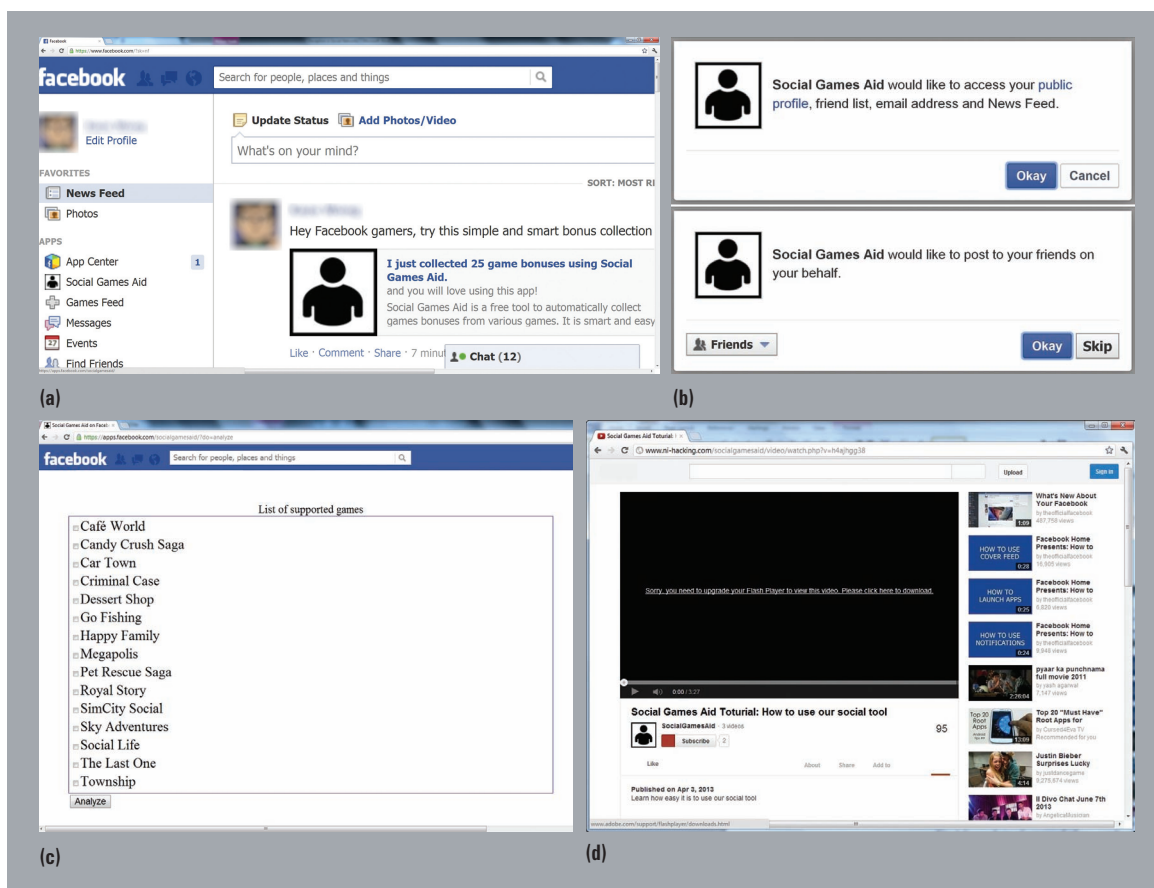
In addition, the fake YouTube site can lead to phishing and botnet attacks.

## Results and Discussions

Our experiment shows how privacy can easily be violated:

- user feeds can be obtained and harnessed;
- friends lists can be obtained to perform social network analysis or to build a larger pool of potential victims;
- phishing can be done by redirecting to a bogus site to further steal users' data; and
- malware can be downloaded to affect users' computers.

As of this writing, 276 people have installed our app. Of those, 97.1 percent have selected the "analyze newsfeed" function, and 27.20 percent have downloaded the potentially malicious software. Furthermore, based on the friends lists secretly taken by our app, we could build a social graph containing 19,763 people, representing a large pool of potential victims. More importantly, we could analyze



**Figure 2.** Screenshots of our proof-of-concept Facebook app: (a) posting an app recommendation to the wall, (b) the malicious app requesting some permissions, (c) the app reading all posts in the users' newsfeeds while "analyzing" the newsfeed, and (d) a user being redirected to a fake YouTube site.

this social network to identify the hub (the most important person), allowing for better marketing or more targeted attacks.

Our experiments have shown that people grant permissions without always understanding what an app can do with them. Users granted permission to our app mainly because they thought the app recommended by us should be trustworthy. Clearly, trust can be abused, creating opportunities for attackers. What happens if someone steals your identity and posts a malicious app to your wall?


By taking a few countermeasures, users can avoid attacks such as the one outlined in our experiment. Before installing an app, users should carefully check what permissions the app requests. If unnecessary or excessive permissions are requested, users shouldn't install the app.

Furthermore, users should

- be mindful when the app is trying to redirect them to another site, because bogus sites can be well disguised;
- validate the URL to avoid accessing phishing sites (in our app, the URL of the redirected video site is [www.ni-hacking.com](http://www.ni-hacking.com), so even though the website looks like a YouTube site, users should be able to identify it);
- review their privacy and security control settings periodically, because social networks often add new features and services that can introduce loopholes and opportunities for attackers; and
- periodically check the information that third parties are accessing.

Users tend to trust the content of requests in social networks, due to their inherent trust of their friends and the social network



platform. However, users need to understand that attackers can easily exploit this trust, despite the technical aspects of their security settings. 

## Acknowledgments

*This work was supported by the Macau Science and Technology Development Fund 039/2010/A.*

## References

1. K.Y. Wong, "Cell Phones as Mobile Computing Devices," *IT Professional*, vol. 12, no. 3, 2010, pp. 40–45.
2. K.Y. Wong, "The Near-Me Area Network," *IEEE Internet Computing*, vol. 14, no. 2, 2010, pp. 74–77.
3. E. Protalinski, "Ice IX Malware Tricks Facebook Users to Enter Credit Cards Details," *ZDNet*, 3 Apr. 2012; <http://www.zdnet.com/blog/security/malware-tricks-facebook-users-into-exposing-credit-cards/11297>.
4. A.A. Hasib, "Threats of Online Social Networks," *Int'l J. Computer Science and Network Security*, vol. 9, no. 11, 2009, pp. 288–293.
5. F. Benevenuto et al., "Detecting Spammers and Content Promoters in Online Video Social Networks," *Int'l ACM Conf. Research and Development in Information Retrieval (SIGIR 09)* 2009, pp. 620–627.
6. H. Gao et al., "Detecting and Characterizing Social Spam Campaigns," *Proc. 10th Ann. Conf. Internet Measurement*, 2010, pp. 35–47.
7. R. Singel, "Hackers Use Twitter to Control Botnet," *Wired*, 13 Aug. 2009, [www.wired.com/threatlevel/2009/08/botnet-tweets](http://www.wired.com/threatlevel/2009/08/botnet-tweets).
8. E. Athanasopoulos et al., "Antisocial Networks: Turning a Social Network into a Botnet," *Information Security*, Springer, 2008, pp. 146–160.
9. J. Kim, "Identity Hijacking on Social Media," blog, Oct. 2012; [www.futureofsocialnetwork.com/2012/10/identity-hijacking-on-social-media.html](http://www.futureofsocialnetwork.com/2012/10/identity-hijacking-on-social-media.html).

**Kaze Wong** is a researcher at the Macao Polytechnic Institute and a graduate student in electronic and information engineering at the City University of Hong Kong. He has finished a number of large-scale government-funded projects on Internet security. His research interests include network security, complex networks, queuing systems, Internet computing, and mobile computing. Contact him at [kazec.y.wong@gmail.com](mailto:kazec.y.wong@gmail.com).

**Angus Wong** is the program leader of the Engineering Sciences team in the Open University of Hong Kong. He has undertaken a number of network-related projects for

the government. His research interests include Internet systems, network infrastructure security, and social network analysis. Wong has a PhD in IT from the City University of Hong Kong. Contact him at [akywong@ouhk.edu.hk](mailto:akywong@ouhk.edu.hk).

**Alan Yeung** is an associate professor in the Department of Electronic Engineering, City University of Hong Kong, as well as a consultant in computer networking and communication systems for government and corporate clients. His research interests include network infrastructure security, mobile communication systems, and Internet caching systems. Yeung is also active in providing consultancy services to local industry in the areas of computer networking and communication systems. His clients include government agencies and listed companies. Contact him at [eeayeung@cityu.edu.hk](mailto:eeayeung@cityu.edu.hk).

**Wei Fan** is a doctoral student in the Department of Electronic Engineering at the City University of Hong Kong. Her research interests include complex networks and social network analysis. Fan has an MPhil in electronic engineering from the City University of Hong Kong. Contact her at [fanwei.fw@gmail.com](mailto:fanwei.fw@gmail.com).

**Su-Kit Tang** is a lecturer at the Macao Polytechnic Institute, Macau. He is also affiliated with the IPv6 Network Research Laboratory in the institute. His research interests include the security of IPv6 network protocol operations, trust and privacy issues in online social networks, and performance improvement in ad hoc routing using network coding. Tang has a PhD in computer science from Sun Yat-Sen University, China. Contact him at [sktang@ipm.edu.mo](mailto:sktang@ipm.edu.mo).



Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.

