



Social Networking Apps Pose Surprising Security Challenges

By Anthony Bettini, McAfee Labs™

Table of Contents

Today's Social Networking Security Challenges	3
Future Social Networking Security Challenges	5
Conclusion	6
About the Author	6
About McAfee Labs™	6
About McAfee, Inc.	6

Facebook, Twitter, MySpace, and LinkedIn—oh my! If we're not using these services ourselves or hearing about them in the media, our friends, colleagues, and children remind us each day of their existence. Although *Web 2.0* may be a buzzword we all love to hate, media-rich web applications that allow information sharing among users are here to stay and growing in popularity. An article written in October 2009 (so it's clearly out of date) on the size of Facebook's data center states Facebook stores approximately 80 billion photos and serves up approximately 600,000 photos per second—making it the largest photo archive in the world.¹ Social networking web applications such as Facebook are a big deal.

As social networking gains users, it will increasingly be targeted by attackers, just as instant messaging and other media have been. For an interesting view on how platform prevalence draws attackers like bees to pollen, see the IEEE article "When Malware Attacks (Anything but Windows)."² One popular technology ripe for exploitation in social network applications is the "mashup." (Wikipedia: "A mashup is a web page or application that uses or combines data or functionality from two or many more external sources to create a new service."³) From the perspective of an application provider such as Google, mashups allow their applications—for example, Google Maps—to become more widely used and embedded within other new applications, like Yelp or the iPhone operating system. However, as we'll soon see, attackers have also been using mashups to their advantage.

Today's Social Networking Security Challenges

"Keep your friends close and your enemies closer" is often cited advice from Sun Tzu, a Chinese general and military strategist who wrote *The Art of War*, around 500 B.C.E. Yet in both personal and business spheres, people rarely do this. From an attacker's perspective, however, this is a common game plan. In the case of a targeted attack—using spear phishing, social engineering, client-side or browser-based zero-day vulnerabilities,⁴ or direct network attacks—the attackers may know more about a bank and its executives than the attackers know about their friends.

Some social networking applications, such as LinkedIn, operate on the premise of "degrees of separation." LinkedIn limits detailed search results to people within your network (which means within three degrees of separation from yourself). Thus, if you were an attacker who wanted to find targets on LinkedIn, you would generally need to be within a few steps of separation from those targets. Users, on the other hand, want to be as far away as possible from attackers.

We've seen evidence of users attempting to increase their search space within a few of the social networking sites. There are various fast ways to do this, such as programmatically adding seemingly legitimate accounts and attempting to automatically link or connect to people. In many cases, users reject requests to link/friend/connect to people they don't know, but some people, such as the "LinkedIn Open Networkers" community, are willing to connect widely, including to people they do not know. Thus users need to be concerned not only with their own connections, but also with their connections' connections—because if the latter link to the attackers, the attackers are that much closer to the former.

What would an attacker do? That is an interesting debate. Regardless, we've seen programmatically generated accounts and link requests, which in effect create a social network botnet. That botnet could facilitate attacks:

- Spam: Some sites include email addresses and share them based on degrees of separation
- Spear-phishing/targeted social networking/emails: These link to sites with unpatched vulnerabilities. The ability to send a message on a social networking service is similar to sending an email, but with far less spam or phishing protection.

1. Facebook now has 30,000 Servers. www.datacenterknowledge.com/archives/2009/10/13/facebook-now-has-30000-servers/

2. Adam J. O'Donnell, "When Malware Attacks (Anything but Windows)," May/June 2008. www.computer.org/portal/web/csdl/doi/10.1109/MSP.2008.78

3. Wikipedia: Mashup [http://en.wikipedia.org/wiki/Mashup_\(web_application_hybrid\)](http://en.wikipedia.org/wiki/Mashup_(web_application_hybrid))

4. 2010 Threat Predictions: www.mcafee.com/us/local_content/white_papers/7985rpt_labs_threat_predict_1209_v2.pdf

- Advanced persistent threats: Everyone’s favorite (or least favorite) buzzword of the year. As social networking exposes private information—job history, friends, birthdays, etc.—persistent attackers may attempt to capitalize on that information.
- Botnet control: Using covert channels

Think I’m imagining things? We’ve already seen Twitter used for botnet commands. Take a look at Figure 1.

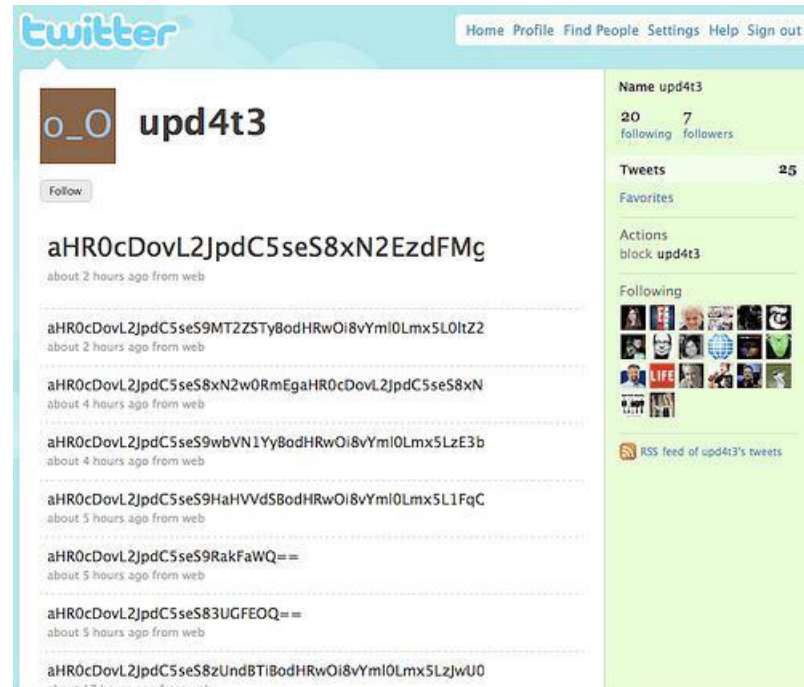


Figure 1: Botnet masters have found that Twitter can serve as a command vehicle.

These scenarios are not just attacks that are likely to happen in the future; these attacks are happening *today*.

One of the best publicized cases of malware exploiting social networking is Koobface (an anagram of “Facebook”).⁵ Koobface uses Facebook messages and wall posts to lure unsuspecting users to websites hosting malware. After a while, Koobface expanded to attack users on other social networking sites such as MySpace and Twitter. As new social networking platforms appear, cases like these are likely to become more common because startups rarely fully implement security. We advise users to open messages and click on links only if the messages are from trusted users and the messages do not look suspicious! In the case of Koobface, the malware was intelligent enough to exploit trust networks and leverage friends to send the links, thus targeted users received messages from people they already knew.

We usually focus on the attacks, but much of the increased ability for attackers to plague our favorite sites is due to decreased privacy. Users too frequently expose their and their employers’ information to social networking applications. Consider a recent mashup whose value, usage, and timing was widely debated in the press. The website, pleaserobme.com,⁶ combined a few elements into a mashup:

5. Craig Schmutz, “Koobface remains active on Facebook,” McAfee Labs Blog. www.avertlabs.com/research/blog/index.php/2008/12/03/koobface-remains-active-on-facebook/
 6. Pleaserobme.com: <http://pleaserobme.com/>

- Foursquare: an application, primarily iPhone-centric, in which users “check in” at various places, such as restaurants
- Twitter: Popular Internet-based, 140-character SMS/Multicast, subscriber-centric instant messaging
- Location-based services

Can you guess the result? As a Foursquare user checked in at a restaurant, a message was sent over Twitter. Pleaserobme.com pointed out that if the users were confirming they were in restaurants and publicly broadcasting that fact via Foursquare/Twitter, then in effect they were telling the world their houses were empty, awaiting a burglar. We could fault the authors of the Pleaserobme.com application mashup, but their purpose was to point out the loss of privacy in using social networking sites in this manner.

Future Social Networking Security Challenges

Given the risks facing social networking applications today, what might we expect in the future? Pleaserobme.com is more likely to represent the beginning rather than the end. In the case of this mashup, it would be easy to expand on that functionality. Instead of simply seeing a user has checked into a restaurant, an attacker could look up the user’s address and map the distance to home from the restaurant. Twitter already provides the city and state in most cases, and Google provides phonebooklike information (street address and phone numbers) for some locations. Thus if the user’s information was present on all sites in question, it would be possible to not only know the distance from home to the check-in location, but also the minimum travel time between the two sites, and possibly a home phone number to call first. A site such as Zillow.com could automatically calculate socioeconomic factors as well.

We’re not trying to give attackers a roadmap. But the ways to expand or iterate on sites such as Pleaserobme.com is obvious from an attacker’s perspective. From a user’s perspective, however, it’s not obvious that checking in at a restaurant and allowing information to remain publicly visible on a social networking site could lead to theft, for example. We want to point out the risks and the ways the dots could be connected. The more awareness users have, the better.

Pleaserobme.com is not the only potential security breach. Triplt is more widely used in the business community than by home users. However, it can also broadcast a similar “I’m not at home” message. Triplt alerts could be used in the Pleaserobme.com example, but there are mitigating factors: Triplt is not widely used, and the alerts themselves are generally less available. For instance, one of the most common ways to see someone’s Triplt alert is for the traveler to link the Triplt alert to his or her LinkedIn profile, and for you to link to that person.

That requires a series of prerequisites to be met, but suppose a VP of sales at a Fortune 500 organization used Triplt on LinkedIn. That VP would send “alerts” on her travel itinerary to all of her linked associates. This may not seem insecure, but a VP of sales at a major corporation would most likely have a vast array of contacts. Some of the contacts would be at competitors, and some of the contacts would not be well known. Further, some small towns in the United States are home to very large companies or major employers. So if a competitor monitored our VP’s Triplt itinerary and saw that she was traveling to a small town that hosts a major potential customer, the competitor could guess that a large sales deal in play or a signing was imminent. This type of business “attack” or intelligence gathering is possibly going on today, but it would be hard to prove. It will be more likely in the future, especially if services such as Triplt become more widespread and more tightly integrated into applications like Facebook, Twitter, and LinkedIn.

Another business-oriented “attack” appears to have already begun to a small degree: using LinkedIn results for corporate recruiting. Posting your resume on Monster.com or Dice.com may not appear kosher while you’re working, but offering your career history (i.e., resume) on LinkedIn (which is basically Monster but with “friends and linking”) is above board and perhaps even *expected*. This is seen as a goldmine in the recruiting world. Now the recruiters have easy access to a candidate’s:

- Name
- Location

- Title
- Job history
- Recommendations
- Number of contacts and perhaps even a list of those contacts

This allows recruiters to very quickly map an organization to find the right candidate for the position they want to fill. In the past some large companies have been hesitant to widely distribute their charts, even within their organizations, fearing that the data would leak to recruiters and their staff would receive recruitment calls.

With LinkedIn, however, org charts have effectively been made public. It would take quite a bit of screen scraping and job-title abstraction to get right, but it might be possible to generate an org chart for a company based only on LinkedIn data.

Conclusion

Like any other Internet technology, social networking needs to have security built in from the beginning. The later security is bolted on to a service, the more costly it will be. As social networking applications continue to evolve, new security challenges will arise. Meanwhile, privacy will decrease as apps request more information and mashups threaten to reveal too much about us. The great flexibility and long reach of social platforms require that we remain more vigilant than ever to protect ourselves.



About the Author

Anthony Bettini is part of the McAfee Labs senior management team. He has also worked at Foundstone, Guardent, Bindview, and as an independent contractor. Bettini specializes in software security and vulnerability detection and has spoken publicly for NIST, the Computer Anti-Virus Research Organization in Europe, RSA Europe 2009, and most recently at the 22nd Annual FIRST Conference on locale-specific threats. He has published new vulnerabilities found in Microsoft Windows, ISS Scanner, PGP, Symantec ESM, and other popular applications. In addition to contributing to a handful of security books, Bettini was the technical editor for *Hacking Exposed, 5th edition*.

About McAfee Labs™

McAfee Labs is the global research team of McAfee, Inc. With the only research organization devoted to all threat vectors—malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based reputation technologies such as McAfee® Artemis™ and TrustedSource™. The McAfee Labs team of 350 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. www.mcafee.com.

