The Threats of Social Networking: Old Wine in New Bottles?

George R S Weir*, Fergus Toolan and Duncan Smeed***

***Department of Computer and Information Sciences, University of Strathclyde, Glasgow G1 1XH, UK.**

****School of Computer Science and Informatics, University College Dublin, Dublin, Ireland.**

ABSTRACT

Despite the many potential benefits to its users, social networking appears to provide a rich setting for criminal activities and other misdeeds. In this paper we consider whether the risks of social networking are unique and novel to this context. Having considered the nature and range of applications to which social networks may be applied, we conclude that there are no exploits or fundamental threats inherent to the social networking setting. Rather, the risks and associated threats treat this communicative and social context as an enabler for existing, long established and well-recognised exploits and activities.

1. Introduction

Can we plausibly regard social networking as a threat? Recent riots in several English cities brought to light the central role played by social networking in co-ordinating mob events. In Scotland, which was free of riots, a number of people were arrested and charged after they used Facebook to encourage gatherings with the aim of rioting. The Glasgow Herald[1] reported that 'two teenagers accused of inciting others to riot using Facebook have been remanded in custody'. One of the two individuals was accused of breaching the peace 'by creating a group on Facebook that could be viewed by the public', thereby, allegedly conducting himself in a disorderly manner by 'inciting others to riot' (op. cit.).

Similarly, a contemporary BBC news report[2] indicated that a 15-year-old boy had been arrested by Northumbria Police on suspicion of incitement to commit damage by using Facebook, and a 21-year-old woman was arrested on suspicion of using a social networking site to incite other people to commit disorder.

These events appear to establish conclusively that there is a threatening aspect to social networking. The arrested individuals (allegedly) broke the law by inciting riots, damage to property and civil disorder. In these particular instances, social network groups were

[1] The Herald, Thursday 11th August 2011, p.3.
[2] http://www.bbc.co.uk/news/uk-england-tyne-14521031

the means whereby the alleged offences were committed. As members of any local community, we may be subject to the effects of such criminal actions. Thereby, any means that facilitates these offences may be considered a threat to life and property.

In this paper, we review key features of social networking and consider the threats that arise from this innovative mode of communication. We argue that computer-based social networking has a dark side, can be dangerous and threatening to individuals and social communities but also that social networking affords no new threats in these contexts. Although social networking may serve as a novel enabler for actions that are criminal, disreputable or simply undesirable, the possible offences are not new. To this extent, we consider the threats associated with social networking to be 'old wine in new bottles'.

2. Social networking

There is an increasing variety of Social Networking Services (SNS) each with a number of common features. Boyd and Ellison [1] define social network sites as

> "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. Of course, the nature and descriptive terms applied to these connections vary from site to site." (p. 211)

Presently, the most popular SNS by far is Facebook which, according to its official statistics, has more than 500 million active users, over half of whom log on to Facebook in any given day. Facebook's own characterisation of a SNS is given in their factsheet:

> "Founded in February 2004, Facebook is a social utility that helps people communicate more efficiently with their friends, family and co-workers. The company develops technologies that facilitate the sharing of information through the social graph, the digital mapping of people's real-world social connections. Anyone can sign up for Facebook and interact with the people they know in a trusted environment."

Other sources of statistics, such as the Inside Facebook data service, have measured growth that shows Facebook will very soon achieve 700 million users.

This paper uses Facebook as the basis for analysis of the threats of social networking. Facebookit is typical of the types of infrastructure that SNSs provide to their users and developers and it is likely to be a long-term survivor in an increasingly competitive

market. Further evidence of the importance of this SNS is the fact that Facebook is now the second most popular site in the world according to Alexa traffic rankings[3].

One important reason for the popularity of SNSs is their emphasis on sharing content and links. In this regard, a recent study has shown that sharing accounts for an estimated 10% of all Internet traffic of which Facebook contributes 38% of all sharing referral traffic that is actually clicked through. If content that is shared but never clicked – the raw numbers – then Facebook actually accounts for 56% of all shared content on the web. This same study also highlights the fact that e-mail now only counts for 15% of shared content – less than half of what it was (34%) in August 2010. Picking up on that last point about the low percentage of shared distributed by e-mail, this is partly accounted for by the fact that amongst 12 to 17 year olds e-mail usage fell by 59% - more than all other age groups' drops combined .

To give further insight into the volume of communications handled by traffic, the official Facebook statistics also reports that more than 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) are shared each month. To support this level of traffic it has been reported by High Scalability[4] that:

> "Facebook has introduced a new Social Inbox integrating email, IM, SMS, text messages, on-site Facebook messages. All-in-all they need to store over 135 billion messages a month."

Given the need to support hundreds of millions of users and hundreds of billions of pieces of content, building the infrastructure for a SNS like Facebook is a monumental engineering effort. The Facebook infrastructure relies heavily on Open Source software technologies and these are listed in the Open Source page for Facebook Developers. In addition to their support for, and adoption of, open source software, Facebook have also started their Open Compute Project, the goal of which is "to build one of the most efficient computing infrastructures at the lowest possible cost… [and] to share these technologies as they evolve." Laudable as these aims are, it does mean that potential exploiters of the infrastructure for nefarious purposes have an insight into potential vulnerabilities that these software and hardware systems may expose.

Even though Facebook is implemented with largely 'open' technologies this does not mean that the Facebook Platform is open and non-proprietary. In essence, SNSs like Facebook are 'walled gardens' that provide their users with features and interactions that are tailored to each user's personal preferences, social graph, and the digital

[3] http://www.alexa.com/

[4] http://highscalability.com/blog/2010/11/16/facebooks-new-real-time-messaging-system-hbase-to-store-135.html

mapping of people's real-world social connections. Therein lies the potential dangers of social networking – the requirement that it captures and stores a user's every message and every interaction with other entities, whether they are other (real) users and/or platform applications that derive their operation, and usefulness, from their ability to extract information about the user from the SNS data repositories and, perhaps, additional data capture and storage on an application-by-applications basis.

Later in this paper we provide specific examples of the types of threat that SNS users are exposed to as a result of vulnerabilities in such systems. These examples will draw upon specific instances that have affected Facebook users but many such threats are generic and apply to other SNSs and, indeed, other web-based platforms such as blogging services and other forms of messaging systems such as Instant Messaging or e-mail.

One aspect of SNSs, in general, and Facebook, in particular, which results in the exposure of users' details to unintended recipients, is the complexity and obtuseness of privacy and permissions settings. This issue comes to the fore on a regular basis and especially when a SNS introduces new features or alters the behaviour of existing features. This has long been a bugbear for Facebook users. For instance, there was considerable furore surrounding the worldwide rollout of Facebook's Tag Suggestions feature (which scans photos and automatically picks out existing friends). Similar concerns regarding the proposal to allow external websites to see users' addresses and mobile phone number resulted in Facebook putting their plans on hold.

Results in a recent study that examined the attitudes and practices of 18 to 19 year old Facebook users by Boyd and Hargittai "challenge widespread assumptions that youth do not care about and are not engaged with navigating privacy"[2]. Nevertheless, Facebook's default settings for permissions and privacy settings can give rise to unintended consequences such as the case of a 16 year old girl's birthday party invite that was sent not only to her connections, but to everyone as a public event and that resulted in 15000 Facebook users RSVPing for the party and an estimated 1500 people turned up despite a cancellation notice being sent out within hours of the original invite.

Aside from the risks that may arise from user error, a service as complex as Facebook is prone to errors of commission or omission. An example of this is the recent revelation that Facebook applications accidentally leaked access tokens to third parties resulting in, for example, advertisers having access to users' accounts including profiles, photographs and messages. Whilst this breach of security was accidental, it has been estimated that at least 20% of Facebook users have been exposed to malware with over 60% of attacks coming from notifications from malicious third-party applications on Facebook's developer platform.

Facebook prides itself on the level of functionality that an application developer can leverage via the Facebook Platform:

> "Building an app on Facebook gives you the opportunity to deeply integrate into the core Facebook experience. Your app can integrate with many aspects of Facebook.com, including the News Feed and Notifications. All of the core Facebook Platform technologies, such as Social Plugins, the Graph API and Platform Dialogs are available to Apps on Facebook.com."

In addition, Facebook's Social Plugins lets user's "see what their friends have liked, commented on or shared on sites across the web." For instance, if a web developer includes a Like Button on a web page then that page becomes equivalent to a Facebook page and a story appears in the user's friends' News Feed with a link back to the web page. Such features are undoubtedly convenient but they do pose a risk. The term "likejacking" has been coined to identify the malware mechanism of clicking on an invisible link that subsequently marks the website as one a user "likes" and which friends see and click on thus spreading the worm to their own news feeds. One reason for the very rapid, viral, spread of such malware is the fact that users are more likely to trust a friend's 'recommendation' in the context of a SNS. Such misplaced trust in the security and integrity of the SNS poses a particular risk to the SNS user base.

The Facebook Platform is also made available to mobile application developers to cater for 250 million users that access Facebook from a mobile device. This introduces further potential attack vectors. For instance, a recent Facebook Mobile API cross-site scripting (XSS) vulnerability caused by insufficient JavaScript validation in the API was used to launch a self-propagating spam worm on the social network.

Facebook is well aware of the types of threat to its service and has mechanisms in place to enlist the help of 'white hats' to identify and report possible security vulnerabilities. This resource is one of a series of pages that highlight Facebook's security policies and, in addition, it provides information and resources about safety on the Internet. There are, of course, third party pages that provide further details of threats to Facebook users, such as the Sophos Security page.

Further efforts by Facebook and others to improve security will see the adoption of OAuth 2.0 and HTTPS as a replacement for older, less secure, authentication systems. Facebook have stated their intention to require all sites and apps to migrate to OAuth 2.0 by October 1, 2011. The reasons given by Facebook for this new policy include:

"As the web evolves, expectations around security change. For example, HTTPS -- once a technology used primarily on banking and e-commerce sites -- is now becoming the norm for any web app that stores user information. We feel that HTTPS is an essential option to protect the security of Facebook accounts, and since Apps on Facebook are an important part of the site, support for HTTPS in your app is critical to ensure user security."

These security-related developments go some way to address one of the steps to better protect users that Sophos has identified in an open letter to Facebook about safety and privacy. Hopefully, such initiatives will help mitigate some of the threats of social networking highlighted in the next section of this paper.

3. Crime and social networks

3.1 Contribution to 'standard' crime

There are many crimes for which no electronic or computing component is required. Examples such as murder, kidnapping, theft, stalking, and chequebook fraud can be committed with no technological ingredients. Of course, while such crimes do not require computers or computer networks, technology-based systems including social networks, can play a role in facilitating these and other common criminal activities.

Social networks provide ideal settings for gathering intelligence and such information may enable criminals to execute their crime, for instance by determining that someone is a 'suitable' victim. This may be illustrated through Scenario 1.

Scenario 1[5]

John uploads a picture to Facebook of his brand new iPad which he has hooked up to his large screen high-definition television. While John may assume that he is only sharing information with his friends. In reality, he may be sharing the information with the world. The scope of visibility for John's Facebook information will depend upon his privacy settings and the security settings for each of his friends' accounts. Since many modern digital cameras embed GPS information in the photograph data, John's posted picture may conceal his precise geographical location and this may be better than a street address for potential thieves, who may conveniently locate the target premises via the GPS co-ordinates.

Mapping software and on-line systems such as Google's street view support the potential criminal who can have a look at the house and its environs before going near the physical location. Google maps (and overhead imagery) may allow the criminal to plan escape routes after the crime. Finally, the criminal needs to obtain a window of opportunity, a time when the house will be vacant. Many users of social network sites regularly update their status,

[5] Cf http://www.telegraph.co.uk/technology/facebook/8004716/Facebook-users-warned-of-burglary-risk.html

including messages to give their friends significant information such as "Having a great time on holiday" or "New York is a fantastic city, you have to visit!". Thus informed, the criminal is able to break-in to the house, steal John's TV and iPad and flee the scene in near perfect safety.

In a real case, 'alleged thieves carried out an estimated 50 burglaries in and around Nashua, New Hampshire, after gaining intelligence on properties that had been left vacant from status updates on social networking sites, such as Facebook'[6]. Warnings against such risks have been also issued in the UK[7].

Some sources suggest that the availability of personal information through social media 'makes lazy burglars happy'[8] while 'users of social networking sites such as Facebook and Twitter could face higher insurance premiums because burglars may be using these resources to discover personal details'.[9] Social media have been used as a setting for intelligence gathering techniques to facilitate many other crimes including murder, sexual assault, child exploitation, fraud, etc. There are evident risks to individuals and organisations through carelessness or ignorance on the part of the social network user. According to Furnell and Botha [3],

> "There are at least two things that users need to understand if they are to properly exert a level of informed control over their social network contributions:
> • The implications of sharing their information.
> • The mechanisms available for restricting access if they wish to do so.
>
> …The initial challenges here are perception, priority and responsibility – essentially requiring the user to recognise that there is an issue to be addressed, that it is important, and that it is down to them to deal with it rather than expecting someone else to take care of it" (p. 14).

In many cases, individuals affected by criminal activity may remain oblivious to the dangerous nature of such 'loose' information, i.e., they may indeed fail to 'recognise that there is an issue to be addressed'.

Of course, social networking tools can work for good as well as evil. Law enforcement agencies have begun to employ social networks as a source of intelligence that allows them to obtain information and catch criminals. In one case, photos of a burglary posted on Facebook by the criminal were seen by the house owner whose home had been robbed and this led police directly to the suspect[10].

For instance, many police forces now have officers who pose as underage children with the aim of detecting child molesters. Hackers have been tracked through social media and evidence gathered that was subsequently used to obtain convictions. There is also a suggestion that Facebook information and social network friendships allowed federal

[6] http://www.theregister.co.uk/2010/09/13/social_network_burglary_gang/
[7] http://www.bbc.co.uk/news/uk-12070679
[8] http://securingourecity.org/blog/2010/12/03/holidays-and-cybercrime-social-media-burglary/
[9] http://www.telegraph.co.uk/technology/twitter/6096677/Facebook-and-Twitter-users-could-be-targeted-by-burglars.html
[10] http://www.wgal.com/news/25953897/detail.html#ixzz1OaeXMEah

agents to establish links between supposed criminals and may have contributed to the arrest of Russians suspected of 'automated clearing house' thefts associated with the Zeus malware.[11]

3.2 Contribution to existing e-crime

E-crime characterises criminal activity in which computer systems or computer networks play a crucial role. Such activities fall into two categories. Firstly, we have offences which are peculiarly associated with on-line activities and are not found outside of the cybercommunity. Secondly, we have offences that are on-line variants of non-technological offences. In the first category we have exclusively on-line scams and social engineering exploits, as well as varieties of computer misuse, such as hacking and malware distribution. In the second category we have on-line variants of non-technological offences, such as cyberstalking, cyberbullying and identity theft.

According to a recent Trustwave global security survey,

> "…the first generation of social networking attacks took a shotgun approach, targeting many users in hopes a small percentage of them would fall victim to the attack. There have been many effective phishing campaigns on Twitter, variants of Koobface have infected millions of Facebook users and social networking sites have been used to expand and propagate botnets. Industry experts have claimed social networking sites are the most targeted vertical in recent years. More recently, attacks have become sophisticated and targeted, through the use of geographical location data and other methods."[12]

Examples of e-crime include scams such as the 'Nigerian 419' and 'Help I'm stuck in London'. These and other exploits potentially benefit from the social engineering influence of social media. In short, social networks can play a role in convincing people to fall for on-line scams. For instance, consider scenario 2.

> Scenario 2[13]
>
> Through a social network, a message arrives from a friend who you know is travelling abroad. The seemingly frantic message advises that they have been mugged in a foreign city and their wallet and passport have been stolen. In order to assist this friend in need, money should be sent via Western Union to a specified account in the remote country where the mugging took place. In this instance, your relationship with the 'victim' (via the social networking site) in addition to your awareness that they are travelling abroad, are social engineering factors that lend credibility to the scam and make you more inclined to send money as aid to your friend.

[11] http://garwarner.blogspot.com/2010/11/minipost-ny-zeus-at-large-codreanu-and.html
[12] https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2011.pdf
[13] http://blogs.pcmag.com/securitywatch/2010/10/help_im_stuck_in_london_and_ca.php

If an individual's account on a social networking site can be compromised (or spoofed) and this opens possibilities to target friends of the victim. As well as the scam described in Scenario 2, unsolicited business propositions from friends are more likely to be accepted than one from total strangers. There is no denying that the success of social networking sites in attracting a mass user base makes the sites themselves a prime target for those who see the users as scam fodder. According to a study conducted by Breach Security, online attacks in the first half of 2009 were up by 30% compared to the same period in 2008, with nearly a fifth of all Web hacking attacks targeted at social networking sites[14]. At least in part, such attacks may aim to gain access to user accounts and exploit the opportunities for socially engineered scams.

The opportunity afforded by social network associations extends to malware distribution. Software coming from a trusted source i.e., a friend stands a good chance of being trusted and executed. If the friend's account has been compromised, the consequences of this trust may be severe and costly.

Malware such as Koobface[15] may also benefit from such trust scenarios, e.g., through automated creation of Facebook accounts, befriending people from these accounts and then directing 'friends' to websites that place malware on visitor's computers. Although the Koobface worm stole account details for social networking sites, rather than directly targeting banking, PayPal or Ebay details, many users used the same credentials on all sites. In consequence, the material loss to affected individuals could have been significant.

Identity theft can arise outside the on-line world, e.g., from information acquired through third-parties[16], but new means are afforded by access to individuals' information on social media. Put simply, there is more personal information available via social networking sites than via any other medium. In consequence, culprits intent on stealing information with a view to identity theft readily view social networking sites as a source of rich pickings.

In effect, social networks afford two means of identity theft. In the first place, they are a source of direct personal information about site members. Often this relies upon the naivety of these individuals in relation to their willingness to expose personal information to public view. For such identity theft, the information readily available on the individual may not be sufficient to accomplish identity theft but it may contribute significantly to the thief's portfolio of personal information about the intended victim. Thereby, the individual becomes more vulnerable to full identity theft, since the would-be thief may use the acquired details to blag further information from a third-party organisation, such as a bank, building society or government department.

The second form of identity theft afforded by social networking is the use of fake personal profiles[17]. In a precedent-setting case, in which an overprotective mother established a fake MySpace identity in order to bully her daughter's rival, the US court ruling has criminalized the act of creating a fake persona online.

[14] https://www.trustwave.com/downloads/whitepapers/Trustwave_WP_Global_Security_Report_2010.pdf
[15] http://news.cnet.com/8301-1009_3-20002112-83.html
[16] http://www.telegraph.co.uk/technology/facebook/8004716/Facebook-users-warned-ofburglary-risk.html
[17] http://www.readwriteweb.com/archives/fake_social_network_profiles_a.php

In such cases, the benefits may be less than full identity theft, since financial gain may be unlikely, but adopting the identity of another person (or organisation) online may provide a means of personal gain or for inflicting reputational damage on the true owner of the stolen identity.

Another worrying trend to which social networks have contributed is the incidence of cyberbullying. Schools are a fertile area for social network usage and some individuals have employed the capabilities of on-line communication to target specific pupils or to spread gossip and rumour against these pupils. Although cyberbullying is not always considered criminal, it can have serious consequences[18].

3.3 New crimes?

Whether there are new crimes associated with social networking is unclear. In order to elucidate the situation, we may distinguish exploits in terms of their victims. In particular, we may appreciate that some social networking activities constitute threats to the public at large, while others represent threats specifically to other social networking users.

3.3.1 Threats to the public

In the former category, are the examples described earlier in which social networking users co-ordinate or encourage mass civil disobedience, rioting and anti-social behaviour. As previously proposed, so far as these activities constitute criminal acts they fall within existing categories of offence, such as 'inciting others to riot', 'disorderly conduct', or 'incitement to commit damage', and do not represent 'new' crimes. Rather, they are recognised criminal exploits that are enabled via social networking activity.

One possible exception to this view is the instance of fake personal profiles on networking sites. The case in which an overprotective mother established a fake MySpace identity in order to bully her daughter's rival, has resulted in a newly defined criminal act of creating a fake persona online. By its nature, this offence, specific to a particular US jurisdiction, only arises in the context of social networking. Perhaps this may be seen as over-zealous judiciary, since the intention behind such a fake persona must be pertinent to the criminality. Indeed, 'spoof' on-line personalities have often been created for comic or commercial objectives, rather than with a view to identity theft or cyberbullying.

3.3.2 Threats to social network users

The majority of 'on-line threats' arising from social networking accrues to other social network users. Social networks afford access to information about individuals. In unforeseen or unconsidered circumstances, such information may provide the ingredients for criminal activity, e.g., identity theft and associated fraud. In this respect, users of social networking sites may be at greater risk of social engineering attacks. The social networking context is by its nature rich in social interaction and affiliation. In turn, this context affords a fertile ground for scams and deception since network users are more apt to believe fellow users (or messages from people who appear to be acquaintances). Once again, social networking serves as an enabler for more effective exploits.

[18] http://www.cbsnews.com/stories/2010/03/29/earlyshow/main6343077.shtml

As noted in a recent Trustwave global security report:

> "Social networks, with millions of users and more people joining every day, are an attractive target for spreading malicious software and information gathering to identify users from a particular company for use in future social engineering attacks. Individuals and businesses should exercise caution in posting potentially sensitive information as well as pay attention to what access levels social "applications" are requesting. Proper education and awareness can help all social network users realize the simple fact that "a friend of my friend is not necessarily my friend."19

The easy one-to-many connection that is afforded by social networks, coupled with the relative anonymity, has also seen them used for child exploitation, including sexual grooming, the generation and dissemination of child pornography.

While these risks may be amplified in the social networking setting, the nature of the exploits is not new. Phishing for personal information, spreading worms, viruses and Trojans, or attempting to groom underage individuals as sexual partners, all aim to commit well recognised crimes that are not specific to social networking.

4. Conclusions

Social networking is now prominent in many aspects of social interaction and can be a considerable force for good. Inevitably, its goals may also be subverted toward crime and other misdeeds.

Our examples in which social networking users may be the targets, illustrate that the networking context serves simply as an enabler in the perpetration of the offence. In the absence of this context, wrong doers would have to find alternative ways to achieve their nefarious ends and, in so doing, would commit the very same criminal acts by different means.

Wherever there is a prospect of financial or other advantage with little personal risk, we will have criminal activity and other varieties of misdeed but at a cost to others. If social networks offer an effective low-cost mechanism to these ends, we should not be surprised to encounter such activities in this environment.

As with any medium of communication, social networking affords a delivery mechanism for good or ill. Scams, extortion, bullying, data theft or incitement to riot, are not new activities introduced with the advent of social networking. In similar vein, we note that the introduction of telephone-based support services afforded 'new' contexts for 'old' offences [4].

On the basis of our survey of social networking exploits and activities, we recognise that most of the undesirable behaviour that has plagued society over the years will re-appear as it is re-enabled by new communication technologies, especially in contexts where the average user

[19] https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2011.pdf

may be innocent and unsuspecting of the threats posed by social networking. Without exception, these threats are merely 'old wine in new bottles'.

5. References

[1] Boyd, D.M. and Ellison, N.B., 'Social Network Sites: Definition, History, and Scholarship'. *Journal of Computer-Mediated Communication*, Volume 13, Issue 1, October 2007, 210–230.

[2] Boyd, D.M. and Hargittai, E., 'Facebook privacy settings: Who cares?' *First Monday*, 2010, 15 [8], 13-20.

[3] Furnell, S. and Botha, R.A., 'Social networks – access all areas?' *Computer Fraud and Security*, May 2011, 14-19.

[4] Moir, I. and Weir, G.R.S., 'Contact centres and identity theft'. *International Journal of Electronic Security and Digital Forensics,* 2 (1) 2009, 92-100.