Cheap and Automated Socio-Technical Attacks based on Social Networking Sites

Markus Huber, Martin Mulazzani, Sebastian Schrittwieser, Edgar Weippl
SBA Research
Favoritenstrasse 16
AT-1040 Vienna, Austria
{mhuber,mmulazzani,sschrittwieser,eweippl}@sba-research.org

ABSTRACT

The vastly and steadily increasing data pool collected by social networking sites can have severe implications once this information becomes available to attackers. Whilst socio-technical attacks such as social engineering relied upon expensive background information collection techniques such as dumpster diving, social engineering attacks can nowadays be fully automated with data collected from social networking sites. In this paper we discuss several socio-technical attacks to finally present a novel large-scale social spam attack based on social networking sites.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection; E.1 [**Data Structures**]: Graphs and networks

General Terms

Security, theory

1. INTRODUCTION

Criminals, as well as direct marketers, continue to clog mailboxes with unsolicited bulk e-mails (e.g., spam and phishing) in the hope of financial gain. So far, their strategy is straightforward, namely to send out a vast number of unsolicited e-mails in order to maximize profit on the tiny fraction that falls for their scams. Their pool of target e-mail addresses is normally based upon data harvested with web crawlers or trojans, sometimes even including plain dictionary-based guessing of valid targets. Previous research indicates that social networking sites (SNSs) might change the playing field of spam attacks in the near future. SNSs contain a pool of sensitive information which can be misused for spam messages, namely contact information (email addresses, instant messaging accounts, etc.) and personal information which can be used to improve the believability of spam messages. A successful extraction of sensitive information from SNSs would result in spam attacks that are based upon a pool of verified e-mail addresses. Thus messages may have higher conversion rates, increasing the success rate of spam.

Gaining access to the pool of personal information stored in SNSs and impersonating a social network user poses a non-trivial challenge. Gross and Acquisti [12] as well as Jones and Soltren [15] were among the first researchers to raise awareness for information extraction vulnerabilities of SNSs. While their techniques were rather straightforward (automated scripts which retrieve web pages), their results eventually led to security improvements of SNSs. Existing attempts to extract information from SNSs focus on the application layer and can thus be mitigated by adapting a specific social network's application logic. Recent publications devoted to information extraction from SNSs introduced elaborate methods such as the inference of a user's social graph from their public listings [4] or cross-platform profile cloning attacks [2]. The leakage of personal information from these platforms creates a remarkable dilemma as this information forms the ideal base for further attacks. Jagatic et al. [14] showed that they could increase the success rate of phishing attacks from 16 to 72 % using "social data". In social engineering, additional available information on targets could lead to automated social engineering attacks [13].

The rest of the paper is organized as follows: Section 2 provides brief background information on social networking sites and research related to security and privacy within these online services. Section 3 outlines various socio-technical attacks based on social networking sites. We explain our main contribution, a possible large-scale spam attack on social networking sites in Section 4. Our findings are finally discussed in Section 5.

2. BACKGROUND AND RELATED WORK

Social networking sites (SNSs) account for today's most popular web services. The main purpose of SNSs is to offer services to foster social relationships and tools to share media online. There exists a number of competing SNSs providers, which Bonneau et al. [5] divided into general-purpose and niche sites. At the time of writing Facebook is the biggest general-purpose SNS with a self claimed userbase of 400 million users [10]. While SNSs are in general accessed via web browsers, SNSs providers started to offer interfaces for access through mobile phones as well.

Social networking sites have been studied in a variety

AISec'10, October 8, 2010, Chicago, Illinois, USA.

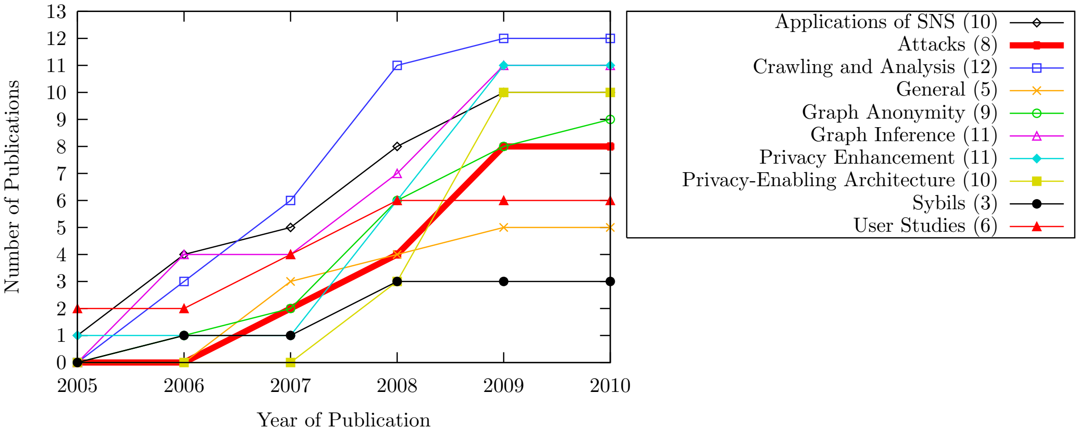

Figure 1: Scientific publications in the area of privacy & security in social networking sites. The publications are divided into different sub-areas to visualize publication trends.

of academic disciplines. Scholars from social sciences have studied the impact SNSs have upon the young generation and their motives to join online social networks [6, 7, 9, 17]. Within the field of computer science, research has been conducted to quantify the size and structure of online social networks [18, 1, 11, 16]. The pool of context information aggregated by social networking sites is of high value for attackers as it is a promising source for malicious attacks. Thus social networking sites have been studied extensively within the area of information security research.

Bonneau compiled a bibliography [3] on SNSs security and privacy which is updated regularly. The bibliography is divided into ten sub-areas (see Fig. 1) and offers in our opinion a valuable summary on research regarding social networking sites' security & privacy. This paper is concerned with SNSs privacy and security attacks (see bold line in Fig. 1) and especially a subgroup of the eight published attacks we refer to as socio-technical attacks. These attacks are discussed in the following section.

3. SOCIO-TECHNICAL ATTACKS

Socio-technical attacks can be seen as the marriage of classic social engineering strategies with technology. In this section we first summarize various attacks based on context-information harvested from social networking sites. In the following we describe automated social engineering bots which make use of an artificial conversational entity (ACE) in more detail.

Context-Aware Spam. Context-aware spam can be generated on basis of data harvested from social networking sites, increasing the effectiveness of the spam. Brown et al. [8] identified three context-aware spam attacks which might be misused: relationship-based attacks, unshared-attribute attacks, as well as shared-attribute attacks. While the first attack is based on relationship information, the two remaining variations use content extracted from social networking sites such as geographic information or a user's birthday.

Social-Phishing. Phishing is a common threat on the Internet where an attacker tries to lure victims into entering sensitive information like passwords or credit card numbers into a faked website under the control of the attacker. It has been shown [14] that social phishing, which includes some kind of "social" information specific to the victim, can be extremely effective compared to regular phishing. For example such information might be that the message appears to be sent from a person within the social environment of the victim, like a friend or a colleague from work. The social graph is therefore not only for the social network operator of value, but for an attacker too, especially if it contains additional information like a valid email address or recent communication between the victim and the impersonated friend. With automated data extraction from social networks, a vast amount of further usable data becomes available to the spammers. Prior conversations within the social network like private messages, comments or wall posts could be used to deduce the language normally used for message exchange between the victim and the spam target. For example, a phishing target might find it very suspicious if the victim sends a message in English if they normally communicate in French.

Automated Social Engineering Bots. Personal information forms the ideal base for social engineering, which exploits the weakest link of IT-systems: the people who are using them. A social engineer tries to manipulate her/his victims into divulging confidential information or performing her/his malicious objectives by using influence and persuasion. Because of the emerging usage of SNSs, the toolset available to attackers is changing, as they can now use SNSs such as Facebook to gather the initial background information on future victims (instead of phone calls or dumpster-diving). [13] demonstrated how context-information harvested from SNSs can be misused in order to carry out sophisticated social engineering attacks in an automated way. Their automated social engineering (ASE) bot makes use of an artificial conversational entity (ACE) based on AIML to communicate with social engineering targets.

4. LARGE-SCALE SPAM ATTACKS

Based on the social aspects of spam and phishing we outline an attack in multiple rounds that tries to spam and phish many people over social networks. We assume that the initial victim can be found over various, commonly available attack vectors for adversaries, like traditional session highjacking over unprotected communication channels or stealing the social network credentials stored in a victim's browser.

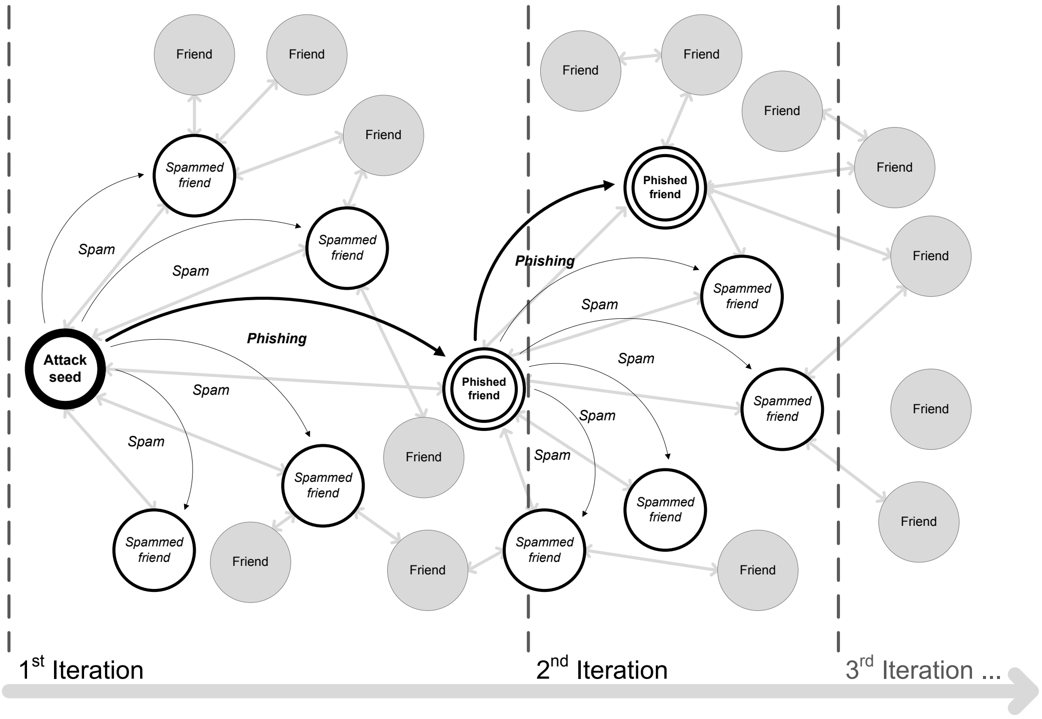

Figure 2: Outline of the large-scale spam attack

Once the adversary is in possession of the account and can impersonate the victim, the following will happen:

1. Retrieve all information needed for the social aspect of the attack, like the list of friends, prior communications or shared events.
2. Send phishing messages to a certain percentage of the victim's friends to continue the "infection".
3. Possibly spam the rest of the friends to maximize profit.
4. Maintain access to the social and non-public profile information, either by installing a custom third party application or adding a prepared "friend" under the control of the attacker.
5. Repeat for the phished friends who fall for the phishing messages, and start the attack cycle all over.

A graphical representation of the different steps of the attack campaign can be seen in Figure 2. All steps can easily be automated. Note that in our attack we either spam or phish a target, as both together may render a victim more suspicious that they fell for an attacker. Furthermore, once we have succeeded in phishing the next victim for the social network credentials, we could use different vectors for spamming like the users stored email address in the social network. This would be very stealthy, as the victim would be unable to connect these two attacks to the same source.

Depending on the attacker's goal, different variations of the attack cycle exist: If the attacker wants to maximize profit by sending as much profitable spam as possible, the ratio of phishing messages decreases as the goal of the attacker is to infect as many different user clusters as possible. If the attacker's primary goal is to collect online credentials (either for continuing the attack or to use the passwords for other online services used by the victim e.g., email accounts), more phishing messages are needed than in the first case. In contrast to traditional computer worms and viruses, it is not efficient to maximize the phishing and spamming rate of every victim, as this would be easily detectable. Targeted and stealth attacks are possible too, by only sending phishing messages to a very small subset of the users friends. We leave that for future work to model and characterize the different attack strategies, with different ultimate attacker goals.

Formal description of the attack in predicate logic. Let $G = (V(G), E(G))$ be a social graph. An edge between two nodes x and y exists iff x and y are friends $F(x, y)$. Friends can access each others context (profile) information $C(x, y)$:

$$\forall x \forall y (F(x, y) \leftrightarrow C(x, y) \wedge C(y, x)) \qquad (1)$$

If an attacker $A(x)$ poses a working security exploit ($exploit$) , she can also access the context information of certain graph nodes (Attack seeds):

$$\forall x ((A(x) \wedge exploit) \rightarrow \exists y (C(x, y))) \qquad (2)$$

An attacker can use context information to spam $S(x)$ or phish $P(x)$ the victim's friends.

$$\exists x \forall y \forall z ((F(x, y) \wedge A(z) \wedge C(z, x)) \rightarrow (S(y) \vee P(y))) \qquad (3)$$

In case the phishing attack was successful $phish(x)$ the attacker can access the context-information of this node:

$$\forall x (phish(x) \rightarrow \exists y (\mathrm{A}(y) \wedge C(y, x))) \qquad (4)$$

The final questions is, how many nodes would get spammed given a certain social graph G, strategy (Σ) and a working security exploit (*exploit*)?

$$\forall x \forall y \forall z((A(x) \wedge F(y,z) \wedge C(x,y)) \rightarrow ((S(z) \leftrightarrow \Sigma(z) = 0) \wedge (P(z) \leftrightarrow \Sigma(z) = 1)) \tag{5}$$

$$\begin{aligned} \mathit{Spammed} : ((V(G), E(G)) &\models \phi(X) \\ \Sigma : V(G) &\rightarrow \{0,1\} \\ 0 &\sim \mathit{spammed} \\ 1 &\sim \mathit{phished} \end{aligned}$$

5. CONCLUSION AND DISCUSSION

In this paper, we briefly discussed various socio-technical attacks against social networks. The previous research in the area of enhanced unsolicited bulk messages such as social phishing and context-aware spam seems especially threatening. We outlined our main contribution, a possible large-scale spam attack on basis of social networking sites. We opine that our outlined viral spam campaign would be cheap to carry out and would have a severe impact. Given the amount of sensitive personal information available from social networking sites in digital form, there are no limits set for cheap and automated attacks. Well established techniques from the area of artificial intelligence could be further used for a number of attacks e.g. for training social engineering chatterbots or using text pattern recognition on harvested personal messages to create tailored spam and phishing e-mails.

Further research

- Estimate the possible impact of large-scale phishing attack on basis of experiments and simulations.
- We believe, that the various proposed security and privacy protection methods do either not scale or do only insufficiently protect social networking users. Hence, further research into protection mechanisms is required.
- A growing number of SNSs users is accessing social networking sites via mobile devices. We believe that this phenomenon needs further research regarding privacy and security implications.

6. REFERENCES

[1] Y.Y. Ahn, S. Han, H. Kwak, S. Moon, and H. Jeong. Analysis of topological characteristics of huge online social networking services. In *Proceedings of the 16th international conference on World Wide Web*, page 844. ACM, 2007.

[2] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda. All your contacts are belong to us: Automated identity theft attacks on social networks. In *18th International World Wide Web Conference*, April 2009.

[3] J. Bonneau. Security and Privacy in Social Networks Bibliography, 2010. [Online; accessed 2010-05-30], `http://www.cl.cam.ac.uk/~jcb82/sns_bib/main.html`.

[4] J. Bonneau, J. Anderson, R. Anderson, and F. Stajano. Eight friends are enough: social graph approximation via public listings. In *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*, pages 13–18. ACM, 2009.

[5] J. Bonneau and S. Preibusch. The Privacy Jungle: On the Market for Privacy in Social Networks. In *Eighth Workshop on the Economics of Information Security (WEIS)*, 2009.

[6] D. Boyd. Why Youth (Heart) Social Network Sites: The Role of Networked Publics. *Teenage Social Life. Youth, Identity and Digital Media. MIT Press, Cambridge, MA*, pages 119–142, 2007.

[7] D.M. Boyd and N.B. Ellison. Social network sites: Definition, history, and scholarship. *JOURNAL OF COMPUTER MEDIATED COMMUNICATION-ELECTRONIC EDITION-*, 13(1):210, 2007.

[8] G. Brown, T. Howe, M. Ihbe, A. Prakash, and K. Borders. Social networks and context-aware spam. In *Proceedings of the ACM 2008 conference on Computer supported cooperative work*, pages 403–412. ACM New York, NY, USA, 2008.

[9] C. Dwyer. Digital relationships in the" myspace" generation: Results from a qualitative study. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 19–19, 2007.

[10] Facebook. Facebook statistics, 2010. [Online; accessed 2010-06-01], `http://www.facebook.com/press/info.php?statistics`.

[11] M. Gjoka, M. Kurant, C.T. Butts, and A. Markopoulou. A walk in Facebook: Uniform sampling of users in online social networks. In *Proc. of the IEEE Infocom*, 2010.

[12] R. Gross and A. Acquisti. Information revelation and privacy in online social networks (the Facebook case). In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 71–80, 2005.

[13] Markus Huber, Stewart Kowalski, Marcus Nohlberg, and Simon Tjoa. Towards automating social engineering using social networking sites. *Computational Science and Engineering, IEEE International Conference on*, 3:117–124, 2009.

[14] T.N. Jagatic, N.A. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Communications of the ACM*, 50(10):94–100, 2007.

[15] H. Jones and J.H. Soltren. Facebook: Threats to Privacy. *Project MAC: MIT Project on Mathematics and Computing*, 2005.

[16] R. Kumar, J. Novak, and A. Tomkins. Structure and evolution of online social networks. In *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, page 617. ACM, 2006.

[17] S. Livingstone. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3):393, 2008.

[18] A. Mislove, M. Marcon, K.P. Gummadi, P. Druschel, and B. Bhattacharjee. Measurement and analysis of online social networks. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, page 42. ACM, 2007.