The dark side of Web 2.0

WA Labuschagne [1,2], MM Eloff[2], N Veerasamy [1]

[1] CSIR, Pretoria, South Africa
{wlabuschagne, nveerasamy}@csir.co.za
[2]School of Computing, Unisa, South Africa
Eloffmm@unisa.ac.za

Abstract. Social networking sites have increased in popularity and are utilized for many purposes which include connecting with other people, sharing information and creating content. Many people on social networking sites use these platforms to express opinions relating to current affairs within society. People do not realize the value of their data divulged on these platforms and the tactics implemented by social engineers to harvest the seemingly worthless data. An attack vector is created when a user can be profiled using responses from one of these platforms and the data combined with leaked information from another platform. This paper discusses methods for how this data, with no significant value to the users, can become a commodity to social engineers. This paper addresses what information can be deducted from responses on social news sites, as well as investigating how this information can be useful to social engineers.

Keywords: Digital Footprint, Facebook, Information Gathering, Internet, LIWC, Social Engineering, Social Media, Profiling, Web 2.0

1 Introduction

Social engineering is the process of manipulating people into performing actions or divulging confidential information which they would not have done under ordinary circumstances. This statement is supported by Mann, author of "Hacking the Human," who defines social engineering as means to manipulate people by deception resulting in them giving out information or performing an action [1].

Numerous studies have indicated that the human element is the weakest link in information security, and cyber criminals have adapted attacks to include this human element [2][3]. Most of the security tools deployed to protect assets within the corporate environment have made it more challenging for attackers to gain access to the corporate network infrastructure. Cyber criminals have adapted to these changes and are adopting social engineering as part of their cyber attacks. The success of social engineering attacks relies on the accuracy of the data collected allowing the attacker to profile the target.

Profiling allows the attackers to predict the behavior of the victims and this is made possible by recording and analyzing the psychological and behavioral characteristics of the target [4]. A social engineer prefers anonymity which results in the search for a

adfa, p. 1, 2011.

platform which stores valuable and collectable data while protecting the attacker's anonymity. Anonymity defends the attackers from any form of network surveillance which could be used to track the location and identity of the perpetrator. Web 2.0 provides such a platform.

In this paper we investigate how cyber criminals could aggregate the posts and comments on a web platform for malicious intent as part of information gathering used during a social engineering attack. In our investigation we test our approach with a proof-of-concept to determine the adverse effects of participation on Web 2.0 platforms like online news websites and social networking sites. Online news websites allow users to express their opinions on news articles, through posts and comments. In addition, users are permitted to participate on news websites using other social networking sites' login credentials which could be used in harvesting additional data about the user.

The remainder of this paper is structured as follows: Section 2 summarizes other research related to profiling and underlying concepts. Our contribution to the research field is discussed in Section 3. Users on social networking sites are not aware of the value of the data they divulge unknowingly. The work in this paper demonstrates how the user's digital footprint could be used for nefarious purposes. User awareness of techniques used by cyber criminals is essential in the protection against threats from cyber space. The findings add to the body of knowledge in the security awareness domain. The implementation follows in Section 4. The findings are discussed in Section 5 and in Section 6 we discuss an example of how the data could be used. Future work is explained in Section 7. We conclude the paper in Section 8.

2 Related Research and Underlying Concepts

This section describes how social engineers could use the digital environment to harvest valuable data as part of an attack. Thereafter a description is given on how the textual data was analyzed before concluding with the potentially nefarious uses of social networking sites by terrorists and infiltration of critical infrastructures using social engineering.

2.1 Digital Environment

Social engineers require information to initiate a social engineering attack. Social networking sites provide a digital platform to harvest and collect data. Social media sites like news websites allow users to post opinions on published articles and comment on posts created by other users. Evans, Gosling and Carroll suggested an individual's personality could be effectively communicated to other users using social networking sites [5]. One of their findings concluded that men are more likely to disclose political views than women. Social engineers could use this information to either build trust with the target or as an emotional trigger. The use of function words within sentences offers insight into the honesty, stability, and self-image of the person

[6]. Furthermore the language use in self-narratives could be used to determine personalities [7]. An investigation by Ryan and Xenos summarized the Big Five and the usage of Facebook [8]. The Big Five are defined as five broad domains or traits of personality used to describe the human personality. The Big Five traits are openness, conscientiousness, extraversion, agreeableness, and neuroticism. For example, neurotic people are easily stressed and upset [9]. This trait can be easily exploited by social engineers.

This iterates the point on gathering reliable and valid information about the target improves the success rate of a social engineering attack. Similarly, the Department of Homeland Security in the United States of America investigated the possibility to predict when terrorist might launch an attack. The predictions were deducted from 320 translations of Arabic of documents released by the terror groups: al-Qaeda, al Qa'ida, Hizb ut-Tahrir, and the Movement for Islamic Reform in Arabia (MIRA) [10].

Social media have been identified as one of the sources from which data can be collected. The following section describes the application used to analyze the data collected.

2.2 Linguistic Inquiry and Word Count

This section provides a brief overview of linguistic analysis and how writing styles can be analyzed. It also describes how terrorists could use social networking sites and how critical infrastructures could be infiltrated using social engineering techniques.

Linguistic Inquiry and Word Count (LIWC) is a probabilistic text analysis program that counts words in psychological meaningful categories. These categories include but are not limited to positive emotions, negative emotions, social words, anger [11]. Consequently LIWC could be used to identify social relationships, emotions and thinking styles from textual data representing human communication. The clarification is made possible by the design of LIWC which consists of two components: the processing components and the dictionaries. The processing component opens a file containing the text and compares each word within the file with the dictionary file subsequently classifying each word to a corresponding category. Next LIWC calculates the percentage for each category. For example consider the following sentence: "*Today is a beautiful day".* LIWC would first take the word "*Today*" and determines if it belongs to one or more categories. The program would increment each of the categories the word is associated with and select the next word until all the words in the file are analyzed. If a word belongs to more than one category then all the relevant categories will be incremented. Consequently LIWC would calculate the percentages for each category for example positive (5%) which implies that the text contains 5% of positive words. The percentage is calculated by dividing the sum of a category by the word count resulting in the following output: function (40%), article (20%), verb (20%), auxiliary verb (20%), present tense (20%), affection (20%), positive (20%), perception (20%), visual (20%), relative (40%), and time words (40%). LIWC has been used in numerous studies, covering a wide range of topics which included predicting deception from textual words [12], identifying gender differences in language

use [13] and the use of language to identify personality styles [14]. It was also used to reveal the psychological changes in response to an attack, for example, the terrorist attack on 9 September 2001 that destroyed the Twin Towers in the United States of America [15].

Style features can also be used to identify writing style. The four major categories of style features are: lexical, syntactic, structural, and content-specific [16]. Lexical features include total number of words, words per sentence, and word length distribution. Syntax refers to the patterns used for the formation of sentences, such as punctuation and function/stop words. Structural features deal with the organization and layout of the text, such as the use of greetings and signatures, the number of paragraphs, and average paragraph length. Content-specific features are keywords that are important within a specific topic domain.

2.3 Terrorists Uses

Terrorists also uses social networking sites. At the University of Arizona Dark Web Terrorism Research Centre, complex models have been built to study extremist-group web forums and thus construct social network maps and organization structures. Research has been carried out to analyze social networking sites but terrorists could also use networking sites to their advantage [17]. Work conducted by Veerasamy and Grobler [18] discussed the different methods used by these organizations for recruitment. The use of profiling techniques could allow these groups to identify potential members based on their psychological characteristics revealed through their expressive writing.

Social networking analysis enables multi-variant analysis which is important for terrorism as the combination of multiple factors: for example, poverty and type of government, combined with the link to a terrorist, may cause a person to participate in a terrorist activity [17]. Thus, using linguistic analysis to gauge these various factors can be beneficial into determining a person's potential to be recruited into a terrorist organization. Furthermore, Ressler says that social network analysis should try to understand the underlying root of terrorism and therefore it is useful to understand how terrorist networks recruit participants and why people join terrorist organizations [17]. By studying the social engineering approaches based on linguistic analysis, insight can be gained on terrorist recruitment practices.

Recruitment could further be extended to include insiders, who are people within companies whom are trusted and have authorized access to valuable resources [19]. The recruitment of insiders employed at critical infrastructure [1] establishments could have devastating effects on the services required to operate a country and could constitute a national security risk. The next section describes the process implemented to protect the identity of the users during the data harvesting.

---

[1] The facilities which are essential for the functioning of a society and economy for example financial services, transportation systems, water supply, public health, etc.

2.4 Method of Data Collection

This study only collected data to demonstrate a possible information gathering phase of a social engineering attack. The only contact made with users was the use of the 'friend request' from Facebook to determine the rate of accepting requests without verifying the true identity and purpose of the request. The friendship was terminated once a request was accepted. Also the data analysis was used to determine potential victims based on emotional response to content; no mechanisms were used to test the findings. No automated tools were used in the data collection as this would transgress the social networking sites the terms of use.

3 Proof-of-Concepts

This section describes the proof-of-concept to determine what data could be gathered from responses on social news sites and how it could be used to conduct a social engineering attack.

The process of a social engineering attack consists of three phases: identify a potential target, data collection to understand and find weaknesses within the target and finally exploit the vulnerabilities identified [20]. This experiment followed the same phases. The design of the experiment involved the manual collection of data from a social media news site, which will not be identified in this paper. The web articles published on this site were selected with the criteria of most responses in the form of posts and comments. This site allows users to post responses to published articles and add comments on posts from other users. Users who would like to create responses are required to login using Facebook account credentials or can create an account on the site.

The user's response in the form of a post or comment can be extracted including the user name and a URL link to their personal profile. The collection process involved the manual capturing of comments and posts from articles published on the site. The collected information does not consist of any personal information except for the URL of the profile which is not revealed in this paper. The collected data were used in two experiments. The first experiment determines what information can be collected using the profile data collected and the second experiment what information can be deducted from the responses created by the users. These two experiments are explained in the following sections.

3.1 Data Collected on Profile Information

A list of all the unique users with their URLs who created responses were compiled from the data collected. Each of the user's profiles was visited to determine how much data was available. A summary was created to illustrate the following categories: visibility of the activities and interests, listing of friends and contact information. The activities and interests could help social engineers in creating a profile about the

user. The summary lists the availability of each of these categories from the public domain (not logged in) and when authenticated (logged in).

The process involved using two web browsers. Facebook was opened in both browsers. In the one browser, which a Facebook user was not logged into, the URL of the collected profile was opened in the browser and subsequently the availability of the required categories was captured. The other browser used the same process except that it used a valid Facebook account and logged into Facebook before opening the collected profile URL. In brief, data was collected about availability of information on a Facebook profile when logged in and not logged in. Next a friend request was send to the collected profiles. The status of the friend request was also recorded. The status conditions are defined as requested, accepted, not enabled and message. There are no responses sent to the requestor if the friendship request is declined, hence no state is created to indicate declined friendship requests.

The different conditions were explained in Table 1. The friend requests are used to determine the current susceptibility of users to accept friend requests without verifying the trustworthiness of the user who sent the friend request.

Table 1. Status Description

State	**Description**
Requested	A friend request has been sent and is pending
Accepted	The friend request has been accepted
Not Enabled	Friend request feature disabled by user
Message	Friend request was not accepted but message was sent from user

3.2 Data regarding Users Responses

The captured responses from the users on the social news website were captured in a database. Some information could be inferred by visiting the profile associated with each user. This experiment analyzes and investigates how the textual responses could be used for profiling as part of a social engineering attack. The data within the database is converted into a text file which is used by LIWC to determine the different emotional dimensions including anger, positive, negative. All of these could be used to determine personality traits. A results file is created once the text files have been processed. The content of the resulting file is extracted and stored in a database which correlates with the previous collected data. This allows the research team to have access to the collected and analyzed data.

Social engineers could use the same process after the collection phase is completed to determine gender. Males have been shown to use more articles (a, the), nouns, prepositions, numbers, words per sentence and use more swear words than females [21]. In this paper we identify negativity and anger as these two emotional states could be employed during a social engineering attack. The use of words could provoke anger in a person which subsequently would prevent the user from making logical decisions [22]. The analyzed data could identify users on social networking sites

who are prone to anger; as the high use of negative and anger words could leak this information unknowingly to cyber criminals.

4 Findings

In this section we describe the results from the experiments conducted. This includes information about the data collection method, the findings from the friendship requests and the analysis of the responses collected.

4.1 Data Collection

The following section describes the finding of the two experiments described in Section 3. A total of 353 unique profiles were listed from the sample collected which consisted of 791 comments and 728 posts from nine articles published on the news website. Data was collected and subsequent friend requests were sent to each user. No additional interactions were conducted after the friend request was sent. A total of 130 requests were sent to users over a period of three days. However, Facebook issued a warning after some users reported the friend requests as suspicious behavior. Consequently, we ceased the friendship requests action. The high acceptance rate was noticed within the first week and then declined after the second week. The collection period spanned over four weeks to ensure that most users had the opportunity to accept the friendship requests sent to them. Security measures implemented by Facebook delayed the collection process using the web browser without having logged into Facebook. Facebook uses mechanisms to identify automated tools and forces the users to prove human behavior with a text challenge e.g. Captcha, before allowing the user to continue. Thus Facebook presents a question and the user must provide a valid answer to be proceed.

4.2 Analysis of Profile Information

This section describes the findings from the information gathered using only the profile URL collected. Findings specifically addressing the friendship requested, are depicted in Fig. 1. At the time of writing the following statistics are available from the data collected. A 35% success rate of friendship requests accepted was obtained from the 130 friend requests sent to the users. Only 4% of users did not enable the “Send Friend Request” feature thus preventing other users from requesting a friendship. An interesting observation is that no users who accepted friendship requests sent messages to request additional information from the unknown user to establish trustworthiness.

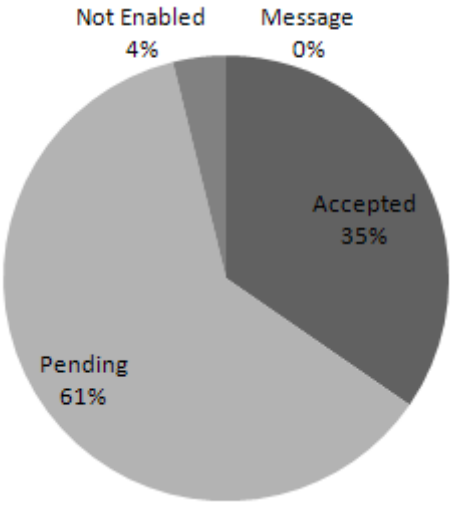
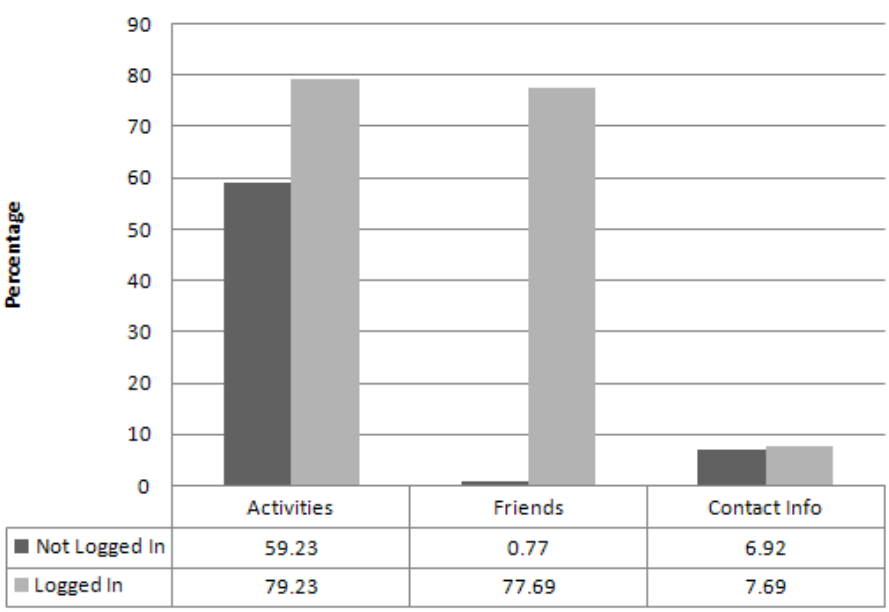


Fig. 1. Facebook Friend Requests

Findings on the data leaked from the profiles are depicted in Fig. 2. Analysis of the data gleaned from the profiles indicates 59% of profiles leak information about interests and activities without the need to log into Facebook. In addition, logging into Facebook and then viewing the profile reveals 79% of interests and activities, an increase of about 20%, compared to the public view of a profile. Equally important is the availability of the user's friends listing which indicates an increase of about 70% of visibility when using a logged in Facebook session. The availability of contact information does indicate a slight increase when accessed through a logged in account.



	Activities	Friends	Contact Info
Not Logged In	59.23	0.77	6.92
Logged In	79.23	77.69	7.69

Fig. 2. Data Leakage

4.3 Analysis of Users Responses

The following section discusses the findings to determine if any users have leaked information which would profile them as prone to a social engineering attack using an emotional trigger. Thus, a form of content-specific writing style analysis was carried out. All the posts and comments were processed to determine the overall average negativity. These include but are not limited to the following negative emotion words: arrogant, ineffective, cheating, outrage and shock. The average negativity of the posts was calculated as 2.9% whereas the average negativity of the comments was calculated as 3.03%. This could be due to human nature where people are more reactive to what other people say or write. Posts were responses on an article which was written impartially. However, comments are responses to bias posts. According to research by Pennebaker, the mean use of negative words in personal text, written to express an opinion, is 2.6% [23]**.** This indicates the existence of posts and comments with a high frequency of negative words.

Fig. 3 provides a graphical representation of the analyzed posts with the mean included. One outlier was identified in the results. The 50% post, upon inspection was a two word sentence with one word a negative word and is subsequently not used in the findings. In addition, numerous posts are clearly more negative than the mean average. The writer of these posts can be classified as potential victims by social engineers. The identity of the potential victim could be extracted from the collected data to initiate an attack. No limiting parameters were utilized during the search hence producing a large potential victim set.

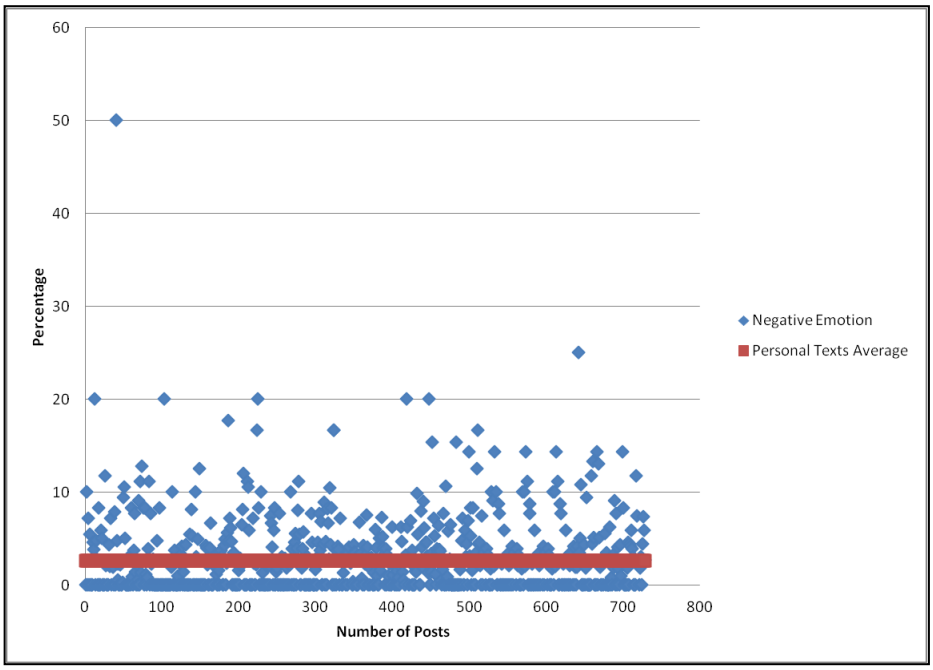


Fig. 3. Negative Emotions for Posts

In addition, the anger dimension was analyzed from the 728 posts collected. The analysis parameters were set to only include posts with a higher percentage than 10%, thus producing a smaller victim pool which will be more susceptible to a social engineering attack (See Fig. 4).

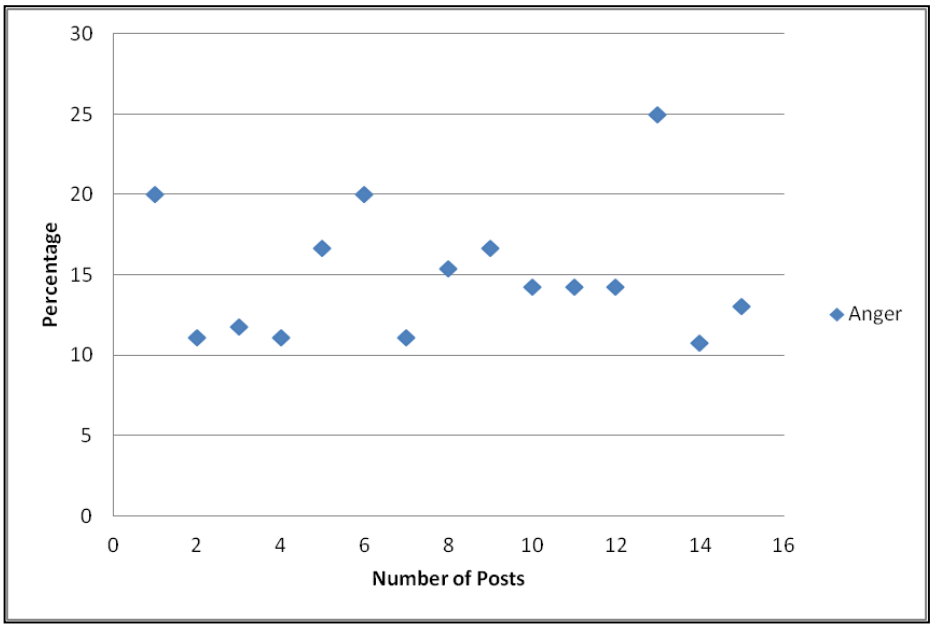


Fig. 4. Anger Emotions above 10%

5 Discussion of the Experiment

In this section we discuss the results found in Section 4 and how the information could be used for malicious intent. Access to users' information could potentially allow attackers to utilize a wide range of methods for nefarious use. Also the collection and analysis of responses could assist in a successful social engineering attack.

5.1 Using Profile Information to Access Additional Data

The information inferred from using only the URL of the user's profile, found users do not understand the mechanisms provided by Facebook to prevent the leaking of personal data. The privacy control settings are continuously updated by Facebook, adapting both to new features developed by Facebook and to the ever changing threat in the environment. However, according to a study by ProtectMyID it was found that only 18% of users implement privacy setting controls [24]. This implies that attackers could easily harvest personal data about users without the need to bypass security measures implemented by social networks.

The results of this study found that more is available when accessing a profile that has once logged onto Facebook. Also most users make public their friend lists which could be used by social engineers to conduct an attack using an evil twin attack. An

evil twin attack is defined as using a rogue profile [2] to impersonate a legitimate profile [25]. The attacker could use data collected from a friend of a Facebook user to create a similar profile to that of the actual friend and subsequently make a friend request. The victim could implicitly trust the source based on the familiarity of the "friend" making the request and information provided with the request which could include a picture and the name of a trusted friend. Another concern raised by the results of this study is the friend request acceptance rate. The study showed that users accept 30% of friend request without asking for additional information.

5.2 Profiling Users

Responses created by users to raise their opinions on current news events could also be used by social engineers. Some of users' personal traits are leaked by expressing an opinion on a specific topic. The use of tools which conduct linguistic analysis could be used to profile a user.

Profiling takes two approaches: prospective and retrospective [26]. Prospective profiling involves the development of a template from previous data. The developed template is then applied to future data to identify individuals whom resemble the characteristics defined within the template. Retrospective profiling uses data left behind to develop a description of the user. In this study retrospective profiling using the data created by the users on the social networking site was used. Such profiling could be used by social engineers to design an attack with elements that improve the probability of a successful attack. The results from the data collected in this study demonstrated how anger and negative emotions could be determined from the responses collected. From this data the attacker could extract the original post that would determine the content which provoked the emotion. This could be then used in designing a customized social engineering attack such as a spear-phishing attack. This attack is targeted towards a specific person or group. The use of this information in a possible social engineering attack is describes in the next section.

6 Application of Data Collected to Conduct a Social Engineering Attack

An attacker could inspect a social news website for controversial articles which have the most responses. Next the attacker collects the data in the form of responses and analyzes these to determine which users have demonstrated the most positive or negative emotions towards an article. These users are classified as victims. The attacker has implicit access to the Facebook profiles of the victims. The attacker uses a fake profile to access data on the individual victim's profile. Results from our study have shown a high probability to access the list of friends. The attacker next uses an evil twin attack and creates a Facebook profile to impersonate one of the friends from the victim's friend list. Next the attacker creates a malicious PDF, naming the file to

[2] Profiles with information which creates a false sense of trustworthiness

correlate with the topic which generated the emotion. For example the analysis showed that the target is negative towards a new tax which will be introduced into the victim's country. The attacker then uses the mail functionality of Facebook to attach the malicious PDF to a Facebook message. The attacker next creates an enticing message using the topic. For example: "*Shocking information leaked about the controversial tax*". The victim will receive the message with the malicious PDF from the fake profile which has the same profile picture as a trusted friend. The victim could implicitly trust the source and then due to the emotional trigger be influenced to open the malicious PDF and infect their systems with malware.

7 Future Work

In this experiment, users were invited to become friends in a social networking site based on a legitimate profile. The experiment will be repeated with the same sample group and the response compared to an invitation from a profile that has minimal information and thus could appear to be an illegitimate user. Thus, a comparative study will be carried out to determine whether users' responses are similar when the profile invitation differs in terms of its degree of legitimacy. This will indicate the need to address the identification of fake profiles on social networking sites.

In addition, this paper briefly introduced the use of linguistic analyses for terrorism recruitment practices. Further research will be carried out to conduct linguistic analyses on social networking sites to determine patterns with relation to content, language and style.

8 Conclusions

In this paper we addressed how users' digital footprints in the form of responses on social news website can be used to create additional attack vectors that could be used to target them.

Two experiments were carried out to determine whether a user could be profiled from their posts on social news sites and also to investigate users' awareness of privacy control settings on social networks. The results show that users can be naive and have a false sense of security which encourages behavior that exposes them to threats. This could be mitigated with security awareness training which allows users to understand the purpose of privacy setting controls and how to implement these to protect personal information on social networking sites. The training could also include other threats that could be encountered on social networking sites for example the evil twin, social engineering and phishing[3] attacks. Furthermore this study showed how emotional triggers that influence users could be determined from responses collected within the public domain. The users should implement strategies to protect their identities on social networking sites which promote freedom of expression. For example, the user could create an alternative profile specifically used to participate on forums

[3] To try to obtain financial or other confidential information from Internet users [27]

which allow users to raise their opinions. These profiles should contain no information which could be used identify the identity of the user.

Both the methods used in this study could be used by social engineers as part of the information gathering phase. The research revealed that information exposed in social networking platforms could be used for nefarious purposes like retrieving personal information, as well as profiling. Furthermore, the personal information that is obtained through the social engineering techniques could be used in an advanced attack vector which combines multiple attack mechanisms to circumvent protective measures implemented to secure a system. In addition, the work has shown that the profiling techniques could be used for malicious purposes like terrorist recruitment and the identification of insiders within critical infrastructure which poses a significant threat to national security. For example, these attackers could target critical infrastructure by identifying possible individuals to infect with malware which targets the critical infrastructure systems or recruit the individuals to join the cause of the terrorist group. These new infected systems or the recruitments could be dormant until action is required by the terrorist group. The access to personal information in the public domain enables these groups to devise strategies to identify and recruit members. These members could be recruited during the planning phase of a possible attack against a country and subsequently become active participants during the execution of the planned attack. Individuals in positions which can cause catastrophic damage to the national security of a country should be cautious of information posted in the public domain. The use of security awareness training that focus on the dangers of personal information in the public domain could provide these individuals with mechanisms to protect themselves against the threats identified. This paper thus aims to create awareness about the dangers of the inference of personal data in the public domain.

9 References

1. I. Mann, Hacking the Human, Gower Publishing Ltd, (2008).
2. C. Carl, "Human factors in information security: The insider threat – Who can you trust these days?" Information Security Technical Report, vol. 14, pp. 186-196, (2009).
3. C. Hadnagy , Social Engineering: The Art of Human Hacking, Wiley, (2010) .
4. D. Shinder. (2010). Profiling and categorizing cybercriminals. Available: http://www.techrepublic.com/blog/security/profiling-and-categorizing-cybercriminals/4069. Last accessed 11 Feb 2012.
5. D.C. Evans, S.D. Gosling and A. Carroll, "What elements of an online social networking profile predict target-rater agreement in personality impressions," in Proceedings of the International Conference on Weblogs and Social Media, pp. 1-6,(2008).
6. C.K. Chung and J.W. Pennebaker, "The psychological function of function words," Social Communication: Frontiers of Social Psychology, pp. 343-359, (2007).
7. J.B. Hirsh and J.B. Peterson, "Personality and language use in self-narratives," Journal of Research in Personality, vol. 43, pp. 524-527, (2009).
8. T. Ryan and S. Xenos, "Who uses Facebook? An investigation into the relationship between the Big Five, shyness, narcissism, loneliness, and Facebook usage," Journal of Computer Human Behavior, (2011).

9. M. Vollrath and S. Torgersen, "Personality types and coping," Personality and Individual Differences, vol. 29, pp. 367-378, (2000).
10. D.Vergano. (2011). Terrorists taunts may tell attack. Available: http://www.usatoday.com/tech/science/columnist/vergano/2011-02-27-terrorist-words_N.htm. Last accessed 27 Feb 2012.
11. J.W. Pennebaker, R.J. Booth and M.E. Booth, "Linqguistic inquiry and word count (LIWC2001): A computer-based text analysis program." (2001).
12. M.L. Newman, J.W. Pennebaker, D.S. Berry and J.M. Richards, "Lying words: Predicting deception from linguistic styles," Person.Soc.Psychol Bull., vol. 29, pp. 665-675, (2003).
13. M.L. Newman, C.J. Groom, L.D. Handelman and J.W. Pennebaker, "Gender differences in language use: An analysis of 14,000 text samples," Discourse Processes, vol. 45, pp. 211-236, (2008).
14. J.W. Pennebaker and L.A. King, "Linguistic styles: Language use as an individual difference." Journal of Personality and Social Psychology, vol. 77, pp. 1296-1312, (1999).
15. M.A. Cohn, M.R. Mehl and J.W. Pennebaker, "Linguistic markers of psychological change surrounding September 11, 2001," Psychological Science, vol. 15, pp. 687-693, (2004).
16. Y.D. Chen, A. Abbasi and H. Chen, "Framing Social Movement Identity with Cyber-Artifacts: A Case Study of the International Falun Gong Movement," Security Informatics, pp. 1-23, (2010).
17. S. Ressler, "Social network analysis as an approach to combat terrorism: Past, present, and future research," Homeland Security Affairs, vol. 2, pp. 1-10, (2006).
18. N. Veerasamy and M. Grobler, "Terrorist Use of the Internet: Exploitation and Support through ICT infrastructure," in Leading Issues in Information Warfare & Security Research, pp. 172-187, (2011).
19. S.E. Goodman, J.C. Kirk and M.H. Kirk, "Cyberspace as a medium for terrorists," Technological Forecasting and Social Change, vol. 74, pp. 193-210, (2007).
20. N. Barrett, "Penetration testing and social engineering: Hacking the weakest link," Information Security Technical Report, vol. 8, pp. 56-64, (2003).
21] J.W. Pennebaker, The Secret Life of Pronouns: What Our Words Say About Us, Bloomsbury Press, (2011).
22. R. Brodie, Virus of the Mind: The New Science of the Meme, Hay House Publisher, (2011).
23. J.W. Pennebaker, C.K. Chung, M. Ireland, A. Gonzales and R.J. Booth, "The development and psychometric properties of LIWC2007," Austin, TX, LIWC.Net, (2007).
24. C. Whitlock. (2011). New survey data from Experian's ProtectMyID™ reveals people are making it easy for cybercriminals to steal their identity. Available: http://www.prnewswire.com/news-releases/new-survey-data-from-experians-protectmyid-reveals-people-are-making-it-easy-for-cybercriminals-to-steal-their-identity-131441283.html. Last accessed 10 Oct 2011.
25. C. Timm, "Evil Twin Attacks," in Seven Deadliest Social Network Attacks, Syngress, (2010), pp. 63-82.
26. N. Nykodym, R. Taylor and J. Vilela, "Criminal profiling and insider cyber crime," Digital Investigation, vol. 2, pp. 261-267, (2005).
27. Anonymous "The Free On-line Dictionary of Computing," (2012).