Threats to computer security with special reference to the exploitation of Social Networks

Louise Kriel, CSIR*, lkriel@csir.co.za;
Elmarie Kritzinger, UNISA#, kritze@unisa.ac.za;
Marianne Loock, UNISA#, loockm@unisa.ac.za

Abstract

The risks associated with placing personal information on a social network are highlighted. This risk increases dramatically if permission is given that allows access to profile information. This risk is not limited to individuals but also to the corporate environment. Computer and personal information security is discussed as well as different security attacks. The potential harm of placing personal information on social networks is discussed. It is demonstrated that personal information as posted on social networks such as Facebook can be readily obtained and stored in a database. Further information can be obtained by utilizing Facebook applications.

Keywords

information, computer security, non-technical, password, phishing, network, software, Facebook, social networks

1. Introduction

Social networks have become prevalent throughout society and are actively used by both adults and children. One of the major social networks is Facebook with nearly 500 million users. Of these users 70% are outside the United States and are distributed throughout the rest of the world with the UK the second largest user group, followed by Indonesia, Turkey and France (Su, 2010). This research proposes to demonstrate a way in which personal information can be extracted from a Social Network such as Facebook and allude to the way in which this can be used for social engineering. The target group for the research was teenagers ranging from 13 years to 18 and for this reason a community, called Fans of Percy Jackson, was established on Facebook to act as the focal point for attracting participants. Percy Jackson is the hero of a series of books by Rick Riordan...
aimed at the targeted age group and the stories have also formed the foundation of a number of films.

Although the target group of the research was people that are generally too young to be employed, the purpose of the research was to demonstrate the danger of placing person information on a social network and allowing people access to it. This holds true for people of any age group and in a technology-dependent environment where information is of paramount importance and many employees are linked to different social networks the risks need to be highlighted. The fact that many employees are active participants on social networks make the management of security more difficult, since the potential access points increase exponentially. Information security can be divided in technical information security and non-technical information security issues. Technical-orientated information security issues focuses mainly technical-orientated knowledge and tools such as encryption techniques that are required to secure and protect information (Smith et al, 2004) and falls mainly outside the ambit of this paper. The non-technical part of information security includes issues such as ethics, legal issues and information security culture (Kritzinger and Smith, 2008).

In order to manage the non-technical risks, they have to be understood. Some of the common risks to computer technology as well as the risk associated with the use of social networks highlighted. Although the term “computer security” is used frequently, a standalone computer is often less vulnerable than a computer connected to a network. As the use of computer networks and social networks have become pervasive, computer security become much more difficult to maintain.

Computer security depends on confidentiality, integrity and availability, represented by the acronym CIA. In addition to technical aspects, the conceptual reach of computer security is broad and multifaceted. Computer security draws from disciplines such as ethics and risk analysis and is concerned with topics such as computer crime; the prevention, detection and remediation of attacks; and identity and anonymity in cyberspace (Kinkus, 2002). The next sections will discuss topics deemed important for the maintenance of computer security.
When asked, internet users often regard privacy as the most important aspect of computer security (Harris Interactive & Westin, 2000; Meinert, Peterson, Criswell & Crossland, 2006). This however does not prevent people from actively using social networks. The development of social networks provides an opportunity to obtain, use or misuse personal (profile) information.

The way in which Facebook functions by providing an Application Programming Interface (API) to allow development of applications for the platform, creates an attack vector. The site allows the extraction of profile information from the users that install and used the application. Facebook indirectly acknowledges this and states the following on their website www.facebook.com:

“While technical and contractual steps are taken to restrict possible misuse of such information by Platform Developers, Platform Developers are not screened or approved and no guarantee can be given that all Platform Developers will abide by such restrictions and agreements”.

“Facebook cannot and do not guarantee that user content posted on the Site will not be viewed by unauthorized persons and no responsibility is taken for circumvention of any privacy settings or security measures contained on the Site.

“All personal information disclosed in a profile or when posted as comments, messages, photos, videos, marketplace listings or other items, may become publicly available.”

More companies store business and individual information on computers than ever before. Much of the information stored is highly confidential and not for public viewing. Many businesses are based solely on information stored in computers. The personal details of staff, client lists, salaries, bank account details and marketing and sales information may all be stored on a database. Without this information, it would often be very hard for a business to operate, and to protect this information, information security systems must be implemented. Facebook offers a starting point to obtain the above mentioned information. When profile information is extracted this provides insight as to where people are employed and often what they are engaged in, both privately and at work. This can give people engaging in social engineering the opening to exploit to obtain both personal as well as company information.

Breaches of information security can be divided into five categories:

1. Interception of messages;
2. Theft of stored data;
3. Information sabotage (i.e. alteration or destruction of data belonging to another party);
4. Spoofing (i.e. using stolen information to pose as somebody else);
5. Denial of service (i.e. deliberate shutdown of cash machines, electric-supply grids, air-traffic control networks, and so on).

Potential individual that may be interested in both personal and employment information are individual computer experts ("hackers"), intelligence agencies, criminals, rival businesses, disgruntled employees and other parties.

Effective information security systems incorporate a range of policies, security products, technologies and procedures. Software applications which provide firewall information security and virus scanners alone are not sufficient to protect information; a set of procedures and systems is necessary to effectively deter access to information (Crystal, 2010). Many of these procedures and security products are rendered ineffective if information to breach security can be obtained. Organizations such as banks try to educate their clients to be aware of phishing attacks. The use of information gained from social networks can be equally or more damaging and at the moment users appear to be less aware of the dangers. In the next section security attacks will be discussed.

2. Social engineering

In computer security, social engineering is a term that denotes a non-technical type of intrusion that relies heavily on human interaction, and often involves tricking other people so as to evade normal security procedures. In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems (Perrin, 2010). There is general consensus that social engineering is a hacker’s clever manipulation of the natural human tendency to trust.

The hacker’s goal is to obtain information that will allow him or her to gain unauthorized access to a valued system and the information that resides on it (Goodchild, 2010). For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get
them to reveal information that compromises the network's security. They might call the
authorized employee with some kind of urgent problem: social engineers often rely on the
natural helpfulness of people in addition to their weaknesses.

An appeal to vanity, an appeal to authority and old-fashioned eavesdropping are typical
social engineering techniques. An attacker may seem unassuming and respectable,
possibly claiming to be a new employee, repair person or researcher, and may even offer
credentials to support that identity. However, by asking questions, he or she may be able
to piece together enough information to infiltrate an organization's network. If an attacker
is not able to gather enough information from one source, he or she may contact another
source within the same organization and make use of the information gained from the first
source to add to his or her credibility.

Social engineering also relies on people's inability to keep up with a culture that depends
heavily on information technology. Social engineers capitalize on the fact that people are
not aware of the value of the information they possess and are careless about protecting it.
Frequently, social engineers will search dumpsters for valuable information, memorize
access codes by looking over someone's shoulder (shoulder surfing), or take advantage of
people's natural inclination to choose passwords that are meaningful to them but can be
easily guessed. Security experts propose that as our culture becomes more dependent on
information, social engineering will remain the greatest threat to any security system.
Prevention includes educating people about the value of information, training them to
protect it, and increasing their awareness of how social engineers operate.

A specific pattern is often identifiable in social engineering. This consists of the four
phases of information gathering, relationship development, exploitation, and execution
(Allen, 2006), illustrated in figures 1 to 5.

During information gathering background information is gathered about the intended
victim. The victim may either be selected randomly because an opportunity is presented to
the perpetrator or a specific victim may be identified. Guarding against becoming a
specific selected victim is more difficult and the sophistication of the attack will to a large
extent determine whether it is successful or not. The best protection remains can still be
achieved by general alertness and adhering to good security practice. To avoid becoming
a random victim the inherent risks associated with the use of social networks, phishing and other forms of social engineering have to be understood. The information gathering phase can be depicted as in Figure 1.

**Figure 1.** Some of the sources used for gathering background information of an intended victim. (Adapted, Allen, 2006).

The next phase in the process is the development of a relationship with the identified victim. This can be done in many different ways such as pretending to share an interest or cause, by direct social contact, social network interaction or in some way gaining the trust of the intended victim. For all of these methods some kind of contact has to be established with the victim and as will be demonstrated social networks present an ideal starting point.
During the exploitation phase the identity of the victim is used to enable the perpetrator to set up the scam. This can be done by opening accounts in the name of the victim, obtaining official documents or any other way in which the perpetrator intends to misuse the information gained from the victim.
During the exploitation phase the actual fraud or scam is executed.

![Diagram showing execution phase]

**Figure 4.** During the execution phase the planned fraud or scam is executed. (Adapted, Allen, 2006).

The fraud can take on many different forms but they all are to the detriment of the victim and to the advantage of the perpetrator. The following are examples:

- Accounts that have been set up in the name of the victim are used for illegal purchases.
- Unauthorized access is gained to proprietary information using the identity and clearance of the victim.
- Illegal transactions in the name of the victim
- Money laundering using bank accounts in the name of the victim
There are different forms of social engineering some of these are discussed in the next.

2.1 Phishing

Phishing is a social engineering technique using apparently legitimate e-mails in an attempt to gather personal and financial information from recipients. It is generally performed by technologically proficient con artists and identity thieves, (Kumaraguru, Rhee, Acquisti, Cranor & Hong, 2007). In a technical deception attack, crimeware designed to steal or intercept a victim’s online account credentials might be used. It can also be used to corrupt local navigational infrastructures to misdirect consumers to false websites (Manning, 2009).

2.2 Smishing

Smishing (short for “SMS phishing”) is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his or her cellular (cell) phone or other mobile device.
2.3 Identity theft

Identity theft is a form of fraud in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. The victim of identity theft (the person whose identity has been assumed by the identity thief) can suffer adverse consequences if he or she is held accountable for the perpetrator's actions. Both organizations and individuals who are duped or defrauded by the identity thief can suffer adverse consequences and losses, and both can be considered victims.

3. Attacks on Social Networks

As the popularity of social networking sites increase, so does their attractiveness for criminals. For example, worms have recently emerged that specifically target MySpace and Facebook users (Darknet Org. 2008). At the moment e-mail attachments tend to raise more suspicion as many e-mail users have experienced malicious mails, they are however not as well-known on social networking sites. Furthermore, incoming e-mails with attachments are often scanned for malicious content and Bayesian filters are applied to sort out unsolicited mails. In comparison, social networking sites do not usually provide filtering mechanisms or warnings for dangerous content, hence, making it easier, in principle, for a potential attacker to send malicious applications and URLs to victims (Bilge, Strufe, Balzarotti & Kirda. 2008). Fortunately social networking sites and services have so far been spared from large-scale, high profile attacks. Nevertheless, social networking sites are an attractive target for attackers because of the nature of the sensitive information that they contain on registered users.

On social networks, users typically enter their real e-mail addresses and provide information on their address, education and professional background, friends, joint friends, activities they are involved in and their current relationship status. Sometimes even previous relationships are listed (e.g., on Facebook, one may read that Mr A’s relationship with Ms B broke up in 2009). From an attacker’s point of view, access to this type of detailed, personal information would be ideal for launching targeted, social
engineering attacks (Jacobsson, 2005). The collected e-mail addresses and personal information would be invaluable for spammers as they would:

- Have access to e-mail addresses that belong to real people. (One problem spammers face is that they often do not know if the e-mail addresses that they collect are indeed being used by real people or they are just secondary addresses that are not regularly read.)

- Have information about the people using these e-mail addresses allowing them to efficiently personalize their marketing activities, tailored according to the knowledge from the target’s profile.

- Be able to successfully bypass spam filters as they will have the ability to associate personal information with an e-mail address. Spam is important to be able to successfully bypass spam filters. Such filters usually generate a list of “spammy” tokens versus “good” tokens after training with a large set of previously received e-mails. As a result, e-mails that contain the name of the user receiving the e-mail, or names of people that he is acquainted with tend to receive lower spam ratings than e-mails that are less personal (Karlberger, Bayler, Kruegel, & Kirda, 2007).

Normally the default setting in Facebook is to allow all confirmed friends to have access to the personal information (e-mail address, photographs, etc.), but not to provide it to unconfirmed third parties. The case study below demonstrates how easy it is to bypass this.

4. Case study

The project can be broken down in discrete parts. Each of these parts was developed and executed in a basic form and then linked with the next as they were developed. During the first phase a Facebook profile was registered for the researcher as well as a web domain.
The next step in the project was the development an interest group page on Facebook with the link to a related PHP quiz (application) that resided on the registered web domain.

Figure 6. Registration as Facebook user and developer as well as the registration of a domain on a public webserver.

Figure 7. A special interest Facebook community with a link to a related quiz that resides on the registered domain on the webserver was created.
During the next step a MySQL database was created on the host and the profiles of people who answered the quiz, login information and their answers to the quiz were stored in the database. When members of the community answered the quiz, they had to allow access to their personal information. Simple data mining, using web based tools could now be performed on the data.

Figure 8. The third party application is linked a MySQL database located on the webserver where profile data and quiz answers are stored. This data can now be used for simple data manipulations.

The last step in the process is to transfer the data from the database on the host to the designated computer where data mining and further analysis of the data can be done as required by the researcher.
Figure 9. Data is transferred to the researcher’s computer as a back-up, data mining and for developing reports. (Adapted, Kriel 2011).

The basic model can be further expanded but was done to demonstrate that this is a realistic way in which identity theft/ misuse can be achieved.

4.1 The quiz

A quiz with questions relating to Percy Jackson was developed and a link placed on the community wall. Members of the community were encouraged to answer the quiz and the link was distributed to ensure traffic over to the community wall. As demonstrated in Figure 3 anyone who wanted to answer the quiz had to allow access to his or her profile information on Facebook in order to be able to complete the quiz. The developed quiz was named “Percy Jackson All Hero Quiz” and as the intention was only to demonstrate the extent to which personal information was obtainable using this route, the questions were spurious and not designed to obtain any specific result.
Figure 10. Link on the Fans on Percy Jackson linking to the quiz.

In Figure 4 an example of the permission to access Facebook profile information that has to be granted is displayed.

Figure 11. Request for Permission to Access Basic and Profile Information

It is during this step that the user grants permission to the researcher that his profile information can be accessed. The application was developed in such a way that this information as well as any answers to the quiz (or any other application) is transferred to a database on the web host.

For this application the data in the database can be displayed as shown in Table 1 below (for privacy reasons this data has been altered and only serves as an example.)
Table 1: Person Table Content

<table>
<thead>
<tr>
<th>Facebook ID</th>
<th>Name</th>
<th>Gender</th>
<th>Date of Birth</th>
<th>Hometown</th>
<th>Education</th>
<th>Date created</th>
<th>Date updated</th>
<th>Email address</th>
</tr>
</thead>
<tbody>
<tr>
<td>60296777</td>
<td>Koos v.d Merwe</td>
<td>male</td>
<td>01/29/1997</td>
<td>Pretoria, South Africa</td>
<td>Menlo Park Secondary School</td>
<td>2011-08-06 10:19:34</td>
<td>2011-08-06 10:19:34</td>
<td><a href="mailto:koos.vd@gmail.com">koos.vd@gmail.com</a></td>
</tr>
<tr>
<td>16154821</td>
<td>John Smith</td>
<td>male</td>
<td>07/13/1996</td>
<td>Cape Town, South Africa</td>
<td>Jan van Riebeeck Secondary School</td>
<td>2011-08-03 09:06:34</td>
<td>2011-08-07 13:50:07</td>
<td><a href="mailto:j.smith@gmail.com">j.smith@gmail.com</a></td>
</tr>
<tr>
<td>50387422</td>
<td>Mandy Bosch</td>
<td>Female</td>
<td>06/07/1998</td>
<td>London United Kingdom</td>
<td>Dunraven School</td>
<td>2011-09-01 16:54:08</td>
<td>2011-09-01 16:54:08</td>
<td><a href="mailto:mmm4@dsy.com">mmm4@dsy.com</a></td>
</tr>
</tbody>
</table>

5. Analysis of data gathered

As the community group has only been functional for a relative short time the number of respondents at the time of the analysis were relatively low. In the first instance the data was grouped in terms of age groups and sex. As the target group for the community was between 13 years and 16 years, narrower band were used for these ages.

As can be expected, the initial respondents were linked to the people that were initially requested to complete the quiz. The first respondents were basically all from the same secondary school. As most of these respondents were in their first year in secondary school the next group to respond were largely pupils who had been in the same primary school as the first group but who attended different secondary schools in the same city. It was interesting to note that pupils whose parents have moved to a different town but still had contact with the pupils who originally completed the quiz also completed the quiz and a number of other pupils at these school completed the quiz as well. After the number of local people who responded dropped and the country of origin of the respondents changed. This can be attributed to the fact that the researcher did not further promote the interest group and the people who responded were people who are interested in Percy Jackson. It was also interesting to note that the age group of respondents did not change and most of these respondents were also between 14 and 16 years of age.
The above mentioned pattern demonstrates the way in which information disseminates on social networks.

Table 2. Age and sex division of respondents of participants completing the quiz on Percy Jackson.

<table>
<thead>
<tr>
<th>AGE</th>
<th>TOTAL NUMBER</th>
<th>NUMBER MALE</th>
<th>NUMBER FEMALE</th>
<th>% OF TOTAL GROUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Below 13 years</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>7%</td>
</tr>
<tr>
<td>From 13 years below 14 years</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>10%</td>
</tr>
<tr>
<td>From 14 years below 15 years</td>
<td>28</td>
<td>10</td>
<td>18</td>
<td>46%</td>
</tr>
<tr>
<td>From 15 years below 16 years</td>
<td>9</td>
<td>3</td>
<td>6</td>
<td>15%</td>
</tr>
<tr>
<td>From 16 years below 18 years</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>7%</td>
</tr>
<tr>
<td>From 18 years below 20 years</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>5%</td>
</tr>
<tr>
<td>From 20 years and older</td>
<td>7</td>
<td>4</td>
<td>3</td>
<td>11%</td>
</tr>
</tbody>
</table>

As can be observed that significantly more girls answered the quiz than boys. This can be a function of the fact that girls at this age (13 to 16 years) appear to spend more time on Facebook than boys. The older people (20 years and older) that have answered the quiz were mostly Facebook friends of the developer. These people completed the quiz as they noticed the activity on the developer’s wall. The response also demonstrate that a specific age group can be targeted the choosing an appropriate subject for the interest group. The subject had appeal in a significant number of countries. At the time of the analysis the respondents were approximately equally divided between South Africa and the rest of the world. This can be expected to change as most of the initial respondents were from South
Africa and the most of the later respondents were from other countries. A breakdown per country of the respondents as can be seen in Table 3 below.

Table 3. The number of respondents per country

<table>
<thead>
<tr>
<th>COUNTRY OF RESPONDENTS</th>
<th>NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>South Africa</td>
<td>30</td>
</tr>
<tr>
<td>United States</td>
<td>11</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>5</td>
</tr>
<tr>
<td>Italy</td>
<td>2</td>
</tr>
<tr>
<td>India</td>
<td>3</td>
</tr>
<tr>
<td>Philippines</td>
<td>1</td>
</tr>
<tr>
<td>Brazil</td>
<td>1</td>
</tr>
<tr>
<td>Kenya</td>
<td>1</td>
</tr>
<tr>
<td>New Zealand</td>
<td>1</td>
</tr>
<tr>
<td>Australia</td>
<td>2</td>
</tr>
<tr>
<td>France</td>
<td>1</td>
</tr>
<tr>
<td>Korea</td>
<td>1</td>
</tr>
<tr>
<td>Ireland</td>
<td>1</td>
</tr>
<tr>
<td>Spain</td>
<td>1</td>
</tr>
</tbody>
</table>

6. Types of data available

Three of the types of data are available from Facebook are discussed next.

6.1 Profile Data

When completing the quiz, the Facebook user allows access to his/her profile information. This is then exported to the MySQL DB on the web host. As can be seen in table 1 this includes gender, birthday (age), town, relationship status and education. This information is updated every time users re-do the quiz or any other application linked to the first one.

6.2 Application of the Data

For this demonstration a quiz was developed and a link placed on the Facebook community page. The questions and the relevant responses are logged into the DB.
Specific applications can be developed in order to target specific groups, or people with a specific profile or to try to obtain specific information or views. This will be more effective if the Facebook community page is also linked to the type of information required, e.g. if the aim is to obtain information about travel preferences, a Facebook community discussing travel destination would draw people interested in this subject. In this instance the Facebook community acts as an initial screening process. It is therefore clear that this type of approach can have different uses:

- Nefarious purpose (highlighted in this paper)
- Obtain market research information
- Ability test (e.g. IQ, technical proficiency)
- Sensitization and support
- Marketing

6.3 Login Data of Facebook User

After the user of the application has given his consent that his profile information can be accessed by the researcher (see Figure 2), this consent stays in place except where the user specifically changes his security settings. It is therefore possible to build up a profile of the user’s login habits such as average login time, the time that the user logs in, e.g. during office hours, in the afternoons or during the night.

7. Information Derived

Three types of information that can be derived from the data available from Facebook, are discussed next.

7.1 Profile Information

The profile information of a Facebook user is the starting point for building up a DB. In itself is of limited use as most people are aware that this information is in the public domain. It can generally be used for categorizing and to perform an initial screening of the user to identify possible targets for further investigation with aims such as corporate espionage or head hunting. When viewing raw profile data it can be observed that a certain percentage of people use aliases and spurious profile data. Typical examples are children younger than 13 years that use fictitious dates of birth and other people who do not want their age to be known.
7.2 Application Information

Application data offers the best source of information as different purpose made applications can be developed to yield specific information regarding the users. These applications can be in the form of a quiz or a game. The data that is collected can further be subjected to data mining to gain further information and to investigate relationships within the data.

7.3 Login Information

Information regarding the login information of user can be obtained from the login data of users. Once a Facebook user has given consent that his profile information can be accessed, all future login details become available. This data can be used to develop a record of the user’s Facebook login information. Facebook users can then be divided into groups in terms of criteria such as total time logged in to Facebook, time of the day that the user normally logs in and out of Facebook. This type of information can be utilized when it is correlated with profile and application information to enhance effectiveness of contact with the user.

8. Conclusion and Future work

Kocher (2006) makes the observation that the most important way of ensuring that information is protected is by making sure that the staff appointed can be trusted and that they are educated properly. The threat of Social Networks to personal as well as company security has to be addressed and user should be made aware of the threat. As society becomes more and more impersonal and the pressure of work keeps on increasing, the need of people to relate to others without maintaining a physical relationship increases. Social network is a phenomenon that will therefore be with us for the foreseeable future. As with any development and technology this will bring both advantages and disadvantages and will lend itself to exploitation by unscrupulous people. In this light the risk associated by allowing personal information to be in the public domain has to be highlighted. In future work the awareness of the public regarding this threat will have to be raised. The current model can be refined and expanded to demonstrate the way in which this information can be linked to other sources on the net.
The Attack Intelligence Research Centre in their 2008 Annual Threat Report predicts that an increase in the amount of Web identity hijacking will be observed and that in response, a serious change in the requirements for validating our identities on the Web will have to be made.

REFERENCES


Bilge, L., Strufe, T., Balzarotti, D. & Kirda, E. (2009). All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. EURECOM Sophia Antipolis, France


