INTERNATIONAL HELLENIC UNIVERSITY

SCHOOL OF TECHNOLOGY

ICT SYSTEMS

DISSERTATION

"Social zombies: modus operandi and countermeasures"

Supervising Tutor: Katos Vasilios

Student: Semkou Athanasia-Maria

November 2013

Abstract

The development and the wide acceptance of the Online Social Networks intrigued many hackers who, taking advantage of the weaknesses in OSNs' systems and the naivety of users by attacking them on a daily basis for profit. The objective of this thesis was to investigate and study this phenomenon and analyze the attackers' "modus operandi", with the aim of automating the detection of Social Zombies. For the purposes of this study, there is a brief review of the social networking development and security and privacy that they provide a description of the attacker's motives. Moreover, a presentation of OSNs' weaknesses and incidents, suggestions for ways of protecting individual users and companies and, finally, a description of a way of using standalone Facebook chats and what they can provide.

Keywords: Online Social Networks, Social Zombies, Bots, Detection, Social Engineering, Facebook, ChatBot, Instant Messaging.

Acknowledgements

I would like to thank my supervisor professor for the opportunity who gave me to work on this interesting topic in the scientific field of my interest, the valuable knowledge and the support that he gave me during the preparation of this thesis. I particularly thank my family for the love, support and contribution over the years of my studies. Finally, I would like to thank Amalia, Giota, Dimitri and Areti for their support over this year of my postgraduate studies.

Table of Contents

Table of Figures

CHAPTER 1: INTRODUCTION

1.1 SOCIAL NETWORK WEBSITES

Since the early years of their creation, social networking websites such as Hi5, MySpace and Facebook attracted millions of people and their involvement with these sites tended to be one of their daily habits. There are hundreds of these sites which have similar technological bases but they attract different social groups of people according to their common interests, their political beliefs, their activities, their common native language, their nationality or their common professional activity. However, these websites differ as far as to the options provided to the user concerned in order to come in contact with his fellows and to share ideas and thoughts. For instance, they can have communication via e-mail, communication via video calls such as the new service of Facebook which was introduced in 2011, chat, writing and displaying personal articles and posting photos or videos.

Figure 1.Social Network Media

Source:http://www.thedrum.com/news/2013/10/12/third-uk-social-media-users-dont-use-facebook-twitter-youtube-flickr-pinterest)

The most popular social networking websites are now Facebook and Twitter which are widely used around the world. However there is a big list of all these services available on the Internet and the most familiar are the following: Nexopia (Canada), Bebo, VKontakte, Hi5, Hyves (mainly the Netherlands) , Draugiem.lv (Latvia), StudiVZ (in Germany), iWiW (mostly in Hungary), Tuenti (mostly in Spain), Nasza-Klasa (mainly in Poland) , XING, Badoo and Skyrock (in Europe), Orkut, LinkedIn and MySpace in South America and Central America and many other (source: Wikipedia).

To be more specific, a social networking site is an online service, whose existence is based on the social relations, offering as motivation for its use the contact with fellows, friends or even family, from every corner of land, pressing only one button. Each user has a profile, which exhibits a large part of his personality and specific personal information such as date of birth, place of residence, school - university - working environment, interests, opinions and photographs. The user, also, has the opportunity through his profile to add a list of other users of the social network and interact with them in ways that differ from site to site. Most web services of this type allow direct communication between users, such as e-mail and chat. In this way, users of the service share ideas, thoughts, music choices and suggestions for upcoming events.

One of the most important advantages of social networking websites is that they offer visualization of these social relationships which may in fact be difficult to achieve in other way. There are users who choose to use these websites just to communicate with people they know and other users on the other hand who use these sites in order to meet new people.

Facebook for instance is the most popular web site on the planet, as it has over 1 billion active users. Facebook is a social networking website launched on February 4, 2004 in which users can communicate through messages with their contacts and notify them when renewing their personal information.

Another social media which is equally popular as Facebook is Twitter. Twitter (Tweeter) is a social networking website which is created in March 2006 by Jack Dorsey and was published in July of that year. The service quickly became popular and now has 500 million users. Twitter allows users to send and read short messages (up to 140 characters), called Tweets. Messages can be read from unrelated users, but only connected can publish texts.

Moreover, MySpace is also a social networking website which is founded in 2003. In August it had 33 million visitors only from USA. Unfortunately, it did not manage to overcome Facebook's visitors and In December 2011, MySpace was ranked 138th to the matrix of visitors.

It is obvious that there many social networking websites which can be particularly referred. One more social media which is very popular is the Foursquare. It is a social networking site basically for mobile phones based on a Geolocation platform. Users can choose from a list of various places and venues and do their "check in" through this application, by winning also as an award some "budgets". The service was created in 2009 by Dennis Crowley and Naven Selvadurai. In April 2012 the service had 20 million users. Foursquare is now one of the most popular applications with the innovative idea: Interaction between people and their environment through their mobile devices.

Figure 2.Social Media

(Source:http://postgradproblems.com/new-study-says-social-media-is-making-you-crazy/)

1.2 DEVELOPMENT

The first social networking website appeared on the Internet in 1997 and was the SixDegrees.com, which allowed users to create profiles, make friends and later to interact with them. However, the ability to create user profiles was already offered to the Internet in dating sites such as AIM, classmates.com and ICQ buddy with the only exception that the user profile was not visible to everybody. SixDegrees.com acquired in a short time millions of users, but did not survive as a business, so the service stopped working in 2000.

Since 1997 to 2001, there have been many attempts by many websites such as LiveJournal, AsianAvenue, and LunarStorm in order to create communication tools among the people. The next big wave of social networking websites came in 2001 with the appearance of Ryze.com, a professional network. Websites like Tribe.net, LinkedIn and Friendster, created and supported by people who personally knew each other and worked professionally, avoiding any competition between them. From the above, only Tribe.net and LinkedIn managed to evolve and be supported by a wide audience, while the Friendster is now considered one of the greatest failed attempts in the online social network era.

Figure 3.Social Website (Friendster)

(Source:http://www.dbswebsite.com/blog/2013/03/06/two-important-lessons-learned-from-friendster/)

Friendster was launched in 2002 to compete a profitable social dating website, the Match.com, considering that friends of each user would suit each other more than with strangers. So the term "Circle of Friends" was introduced in social networking. This site was acquired very soon millions of users and attracted many investors. However, as its publicity was increasing, many technical problems appeared in terms of data capacity,

but also social as many users had to "deal" and their bosses, along with their closest friends. So Friendster started to limit users' ability until Fakesters came up. There were people who created fake profiles so as to make many friends and access their profiles. So the service proceeded to automatically expulsion of members with profile pictures which seemed fake. All this slowly led to the "collapse" of this website from the top of the pyramid of social networks. Despite this, we should mention that is still used mostly in Asia and in the Philippines.

Since 2003 and then, many social networking sites have appeared on the Internet. Each one of these sites targeted in specific groups of people, such as the Couchsurfing, which was created for people who love to travel, MyChurch for those who believe in religion, the LinkedIn, Visible Path and Xing for professionals, and so on. LinkedIn now has over 30 million members. Moreover, similar websites have created, which support media sharing such as Flickr, YouTube and Last.FM.

After all these, two great companies, Microsoft and Google created their own social networking websites MSN Spaces and Orkut respectively. In 2003 the website MySpace made its appearance which was a clone of Friendster. It started working after only 10 days of programming, and it used for profile creation and promotion for rock bands. The friendships between the bands and their fans, created through MySpace, contributed substantially to its growth. A pioneering move in this social networking website was that the users could form their profiles as they wanted because it supported HTML code.

The creation and the expansion of social networks had continued for many years worldwide. Each country has its own culture, so it has its own Social Networks. For instance, the Chinese messaging service "QQ" became a huge social network in Korea, and later added the service profiles for its users, the possibility to apply for friendship and a conversation tool the Cyworld.

Having all these social networks came another one, named Facebook. Facebook was first used as a networking service from students at Harvard. In September 2005, it was expanded, including users such as high school students, professionals and in 2006 people from all over the world. The dominant feature of the site was the existence of closed networks for all; open only to persons directly concerned to them. Facebook did not allow user profiles to be publicly visible to everyone. It also gave the opportunity to developers to build applications which would

allow users to create polls about music, to play games through them and so on.

In 2006, Twitter made its appearance on the Internet and promoted to the general public a new form of social networking, the micro blogging. Users have the opportunity each time to be connected to it either by mobile phone or by computer and also to inform their contacts for their everyday occupation in real time by answering the question “What are you doing at the moment?” which has integrated on its website. Twitter has censored many times for the fact that if retains its capacity to keep everyone in touch or just finally informs about what people make every minute. A clone of Twitter is the Jaiku which was supported by Google for two years but now its future is uncertain.

In the community of social networks was recently added on June 28, 2011, the Google Plus, which is now available to the public. The similarities with Facebook are many. It allows users to share photos, links, videos and so on. However, its big difference is that it simulates the interpersonal relationships as they are in reality. In Google Plus appears a new term, the “Circles” which is created based on the status of each individual, allowing the user to selectively share different things with each of his circles. Google Plus also allows users to edit the images or videos and simultaneously talking via chat more than 10 friends, applying Hangouts. Apparently, Facebook has a new competitor and only users will reveal the winner of this "battle."

We should also mention the every user of the Internet is able to create his own Social Network via the Ning platform.

Finally, it is worth to put some graphics concerning the development of the bigger social networks, with which we will deal in the context of this thesis, Facebook and Twitter. It is widely known that Facebook has turned into a giant of billions company, with more than 500 million active users and its development which is faster even from Google.

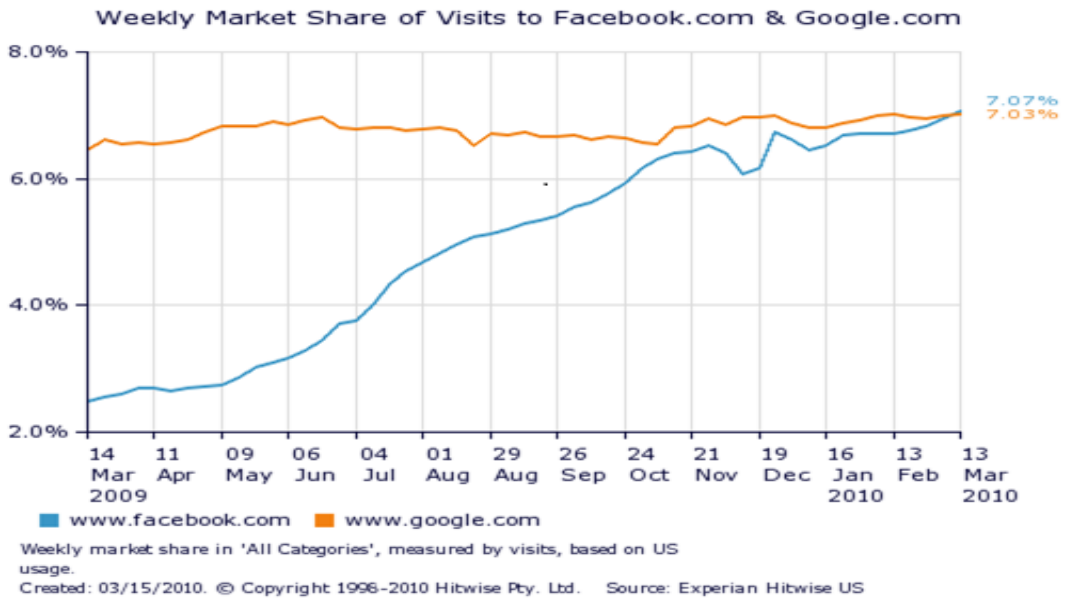
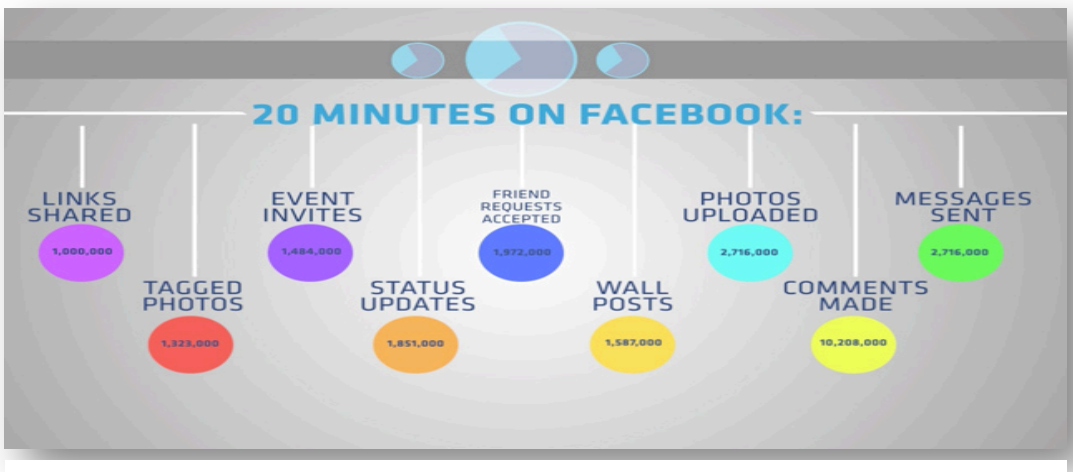


Figure 4.Weekly Market Share of Visits to Facebook & Google

(Source:http://www.jwtintelligence.com/2010/03/data-point-social-is-the-webs-new-queen-bee/#axzz2iwnBxZyt)

The most impressive of all, is the fact that the users' total upload for the New Year was 750,000,000 photos, while according to the following chart every 20 minutes on Facebook users make 10 billion comments and send over 2.7 private messages . Watching the numbers, it is obvious the world's obsession with this social network and the important role it now plays in people's life.



(Source:http://tommytoy.typepad.com/tommy-toy-pbt-consultin/2011/03/infographic-how-the-entire-world-has-become-addicted-to-facebook-zuck-is-your-master-people.html

As far as Twitter concerned there are some interesting facts concerning its growth. From these facts we understand that Twitter has become one of the favorite daily habits in the world.

- It was needed 3 years, 2 months and 1 day to overcome the 1 billion tweets. Nowadays, it is needed only 1 week to reach this number.
- One year before the users sent approximately 50 million tweets per day and the last month the number was 140 million tweets.
- On 12 March 2011 there were created 572,000 new accounts.

All the same, this enormous growth of social networking websites and the role that they play in our lives affected our society in various fields. As regards education, the University of Salford has announced that it will create a new postgraduate program, which will likely bring the title "Master in Social Media", and it will offer specialization in Social Networks. Furthermore, it is observed that except from people, many radio and television stations and newspapers - magazines have created their own pages or applications to provide information via social networks. The stores also have created their own website in online social networks which hold competitions to convince users to visit them and to be advertised. We have to mention that in some countries like China, citizens are not allowed to have access on Facebook and Twitter. On the contrary of that, in Greece even the Prime Minister and Police support them and also have accounts on Twitter in order to inform our citizens.

Finally, it is important to be mentioned that according to a survey conducted by the company Consumer Reports, 1% of Facebook's population is consisted of children 10 to 13 years and their number stands at 7.5 million, which violates the terms of service as well as the use is allowed to people over 13 years. With these conclusions we have to start to concern. Now it remains to see where this technological modernization will lead and how will affect our lives.

1.3 PRIVACY

The wide acceptance of social networking websites from the world had also resulted in the publication of many personal data on the Internet. The Social Networks, exploiting the trust of their users, they now gather information from people who have an account. When a user signs up to a social networking website, he is able to answer questions provided by the service to create his own personal profile. These questions are related to the following: date of birth, place of residence, place of origin, school, university/workplace, phone number, e-mail account, religious and political beliefs, interests, favorite music/movie/book and personal relationships with other people. Besides all these, the user is encouraged to publish personal photographs in order to make his profile more recognizable to other users.

After an extend survey on the Internet it is observed that the social media continuously grow but their privacy and their secure decreases. A good example is the changes that occurred in the already settings on Facebook, concerning the privacy of our personal data. We should say that all the users' personal data are available on the Internet. According to a research company "Consumer Reports", one to five Facebook users has never set the security settings of his account and therefore do not know how to protect his personal data.

A very good example which caused big surprise to the international community was the case of a law student from Austria. Furious as he was with the security settings of Facebook and based on the European legislation, required from the service to deliver all the data concerning him. Max Shrems surprised accepted a CD with 1,222 files PDF which included all his personal details and pictures that he had posted, all the friend requests that had been accepted or rejected, all the "likes" that had done, profiles of friends whose had visited, the number of how many times he had seen some pictures, his preferences in products, his discussions via chat and all these data that he had deleted. After this incident, the 24 years old student started a campaign, which was called "Europe vs. Facebook" and its aim is to "wake up" people concerning the vague privacy policies in social networking services.

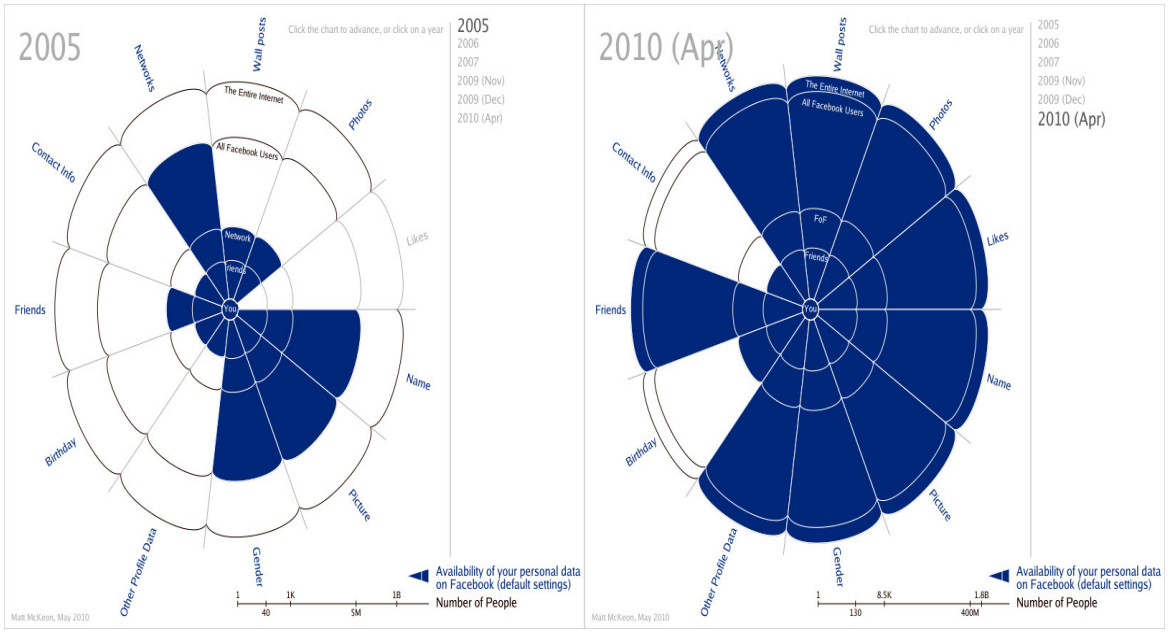


Figure 6.The Evolution of Privacy on Facebook

(Source:http://www.yalelawtech.org/control-privacy-technology/evolution-of-facebook-privacy/)

Apart from the users' data on their profiles on Facebook, it is known now that this service keeps a back up history from all its users even if they are connected or not. It knows every web page that they visit and keeps mind of it even though the user does not stay or do something in this web page. So, Facebook knows whatever users do on the Internet. The administrators of Facebook claim that all these data are used only for research purposes, so that Facebook can improve its plugins. However, the information that they have, it can be easily exposed to third parties and users cannot do anything.

Furthermore we should concern on how the naïve use of these kinds of websites may also affect our professional career. According to reports on the Internet, there is a service in California named "Social Intelligence Hiring" which has created in order to help companies to recruit new employees, providing them information that can be gathered from social networking sites and blogs, with the help of automated detection tools. This information concerns mainly data which is publicly visible and it is not allowed to be included sensitive personal information in reports such as the user's age, religious beliefs and so on. Through these reports, companies look for suspicious posts, for example by using users' gallery, so as to find likely consumption of alcohol or other substances and make sure for a successful recruitment. So beyond the checking of the general

background of the employees and their criminal record, it is also now important their Internet business. It was recently reported in Britain and according to a decision of the British court that any user tweet on Twitter is publicly visible; it can be used by the press.

On January 2012, Google announced that it will create a new search service called "Search, plus Your World". The service will display content of user accounts of Google+, even data that have been figured to not be visible to everyone. Twitter had already implemented with the appearance of users' Tweets in search results. Apart from Google, the founder of Facebook Mark Zuckerberg had also announced the integration of a new messaging system, which is a real-time system that collects all messages that can a user accept such as SMS, Facebook messages, chat, emails. This venture will facilitate and take complete control of communication that a user will have with his fellows and is now provided to all users with the form of an e-mail address: username@facebook.com.

So it is completely obvious and understandable from everyone that from all these that were mentioned above, there are serious issues in terms of ethics and privacy which have to be taken into consideration by all of us.

1.4 SECURITY

The social networking sites based on human relationships and communication, encourage their users to post more and more personal information to them. So the users based also on their will to make impression on their friends, trust and follow any prompts of these services, which guarantee them with anonymity on the Internet, the sense of security through their communications and that their personal information are visible only to their friends. Direct consequence of the above is to consider the social networking websites as a goldmine for launching attacks social engineering by cybercriminals.

According to the theory of computer security systems, a service is considered safe if it respects the security triad: Confidentiality, Availability and Integrity. However, in social networking sites confidentiality is violated when the attacker gains access to data without being authorized by the owner, integrity when the unauthorized attacker can modify the state of the user's account or any information in this and finally the availability may be violated when the access to accounts is not permitted to authorized users of the service due to the intervention of the attacker. Therefore, we end up that the online services do not provide the required security for their users.

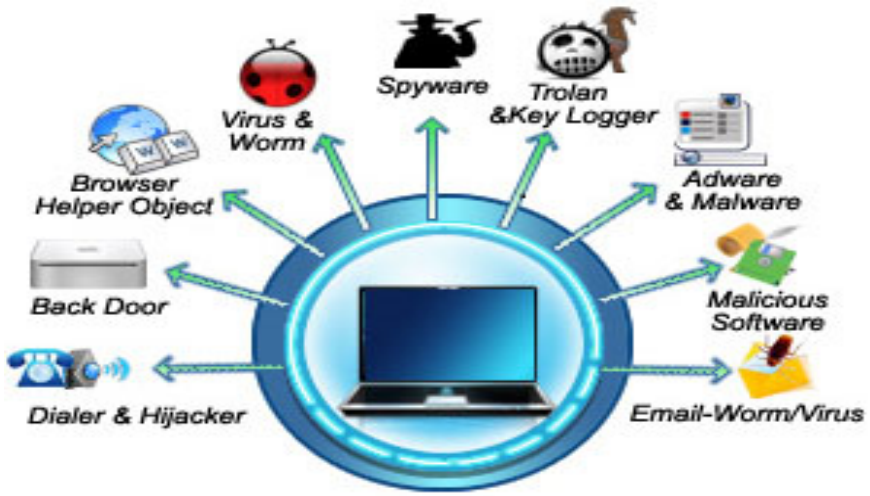


Figure 7.Malwares

(Source:http://fullonn.blogspot.gr/2011/07/computer-security-threats-malicious.html)

The attackers exploit the weaknesses of the websites and having also the trust of the users, they proceed to malicious actions which their main purpose is the profit. However, they focus mainly on Social Networks that considered the most popular and widespread and with many registered users. Many of our examples will be mentioned on Twitter and Facebook as they constitute the two main targets for the cybercriminals. The attackers through various persuasive tricks such as spam messages try to fool a large percentage of users and achieve their illegal purposes by simply "putting" malware files to the computers. Some of these malwares are the viruses which are harmful programs that are activated by specific files and infect the system files. Other types of malware are the worms which are harmful programs that are automatically play through the network, the spyware which is used to monitor the activities of the infected computer and the adwares which are programs that show to users advertisements without his permission and slow down the speed of the network.

Last but not least, the trojan horses which are malicious programs that seem harmless but they alter the function of the system so as to gain access in it.

It should be mentioned that everyday 4 million Facebook users receive spam messages and 6 thousand users are victims of deception. However, Twitter has only received 12 severe malicious attacks and the last one was in 2010.

CHAPTER 2: LITERATURE REVIEW

2.1 SOCIAL ZOMBIES

Social (Media) Zombies, a term recently defined (2009) by *Tom Eston* and *Kevin Johnson* and it was used in their presentation entitled "Social Zombies: Your friends want to eat your brains", in the conference DEFCON 17. The main topic of this presentation was the social networking websites as well as security and privacy that they provide. The two above researchers along with Robin Wood came back with one more presentation named "Social Zombies 2: Your friends need more brains" in the conference ShmooCon (2010).

This term has caused great sensation to everyone in the conference and generally to the public. So with the term "social zombies" we mean the computers which are infected by specifically designed software and are used from unauthorized users for malicious purposes. The software is implanted into the computer (Social Zombie) by means of a social web network, such as Facebook, or Twitter and so on.

Figure 8.Social Media Zombies

(Source: http://www.tinkernut.com/gallery/)

The computer user is contacted via infected email or other social communication, a process during the user's computer is infected and turned into a social zombie.

2.2 BOTS

Another name for the social zombies is **Bots**, which comes from the word Robots. The Bots or Social Zombies, usually form a whole network of controlled computers the **Botnet** (Robot Network). The purpose of the formation of a botnet is to give to a person or a team of people the control over others people computers and accounts, with the computer or account holder having lack of knowledge of such control.

The botnets can be divided into 3 categories according to the type of control. Centralized bots are those where the control is located to a central server the C&C (Command-and-Control). The decentralized bots are those where the control is not given by a C&C and distributed botnets are those where the control is literally distributed among many social zombies. They operate based on commands so as to implement their goals for people who are known as "botmasters" or "botherders".

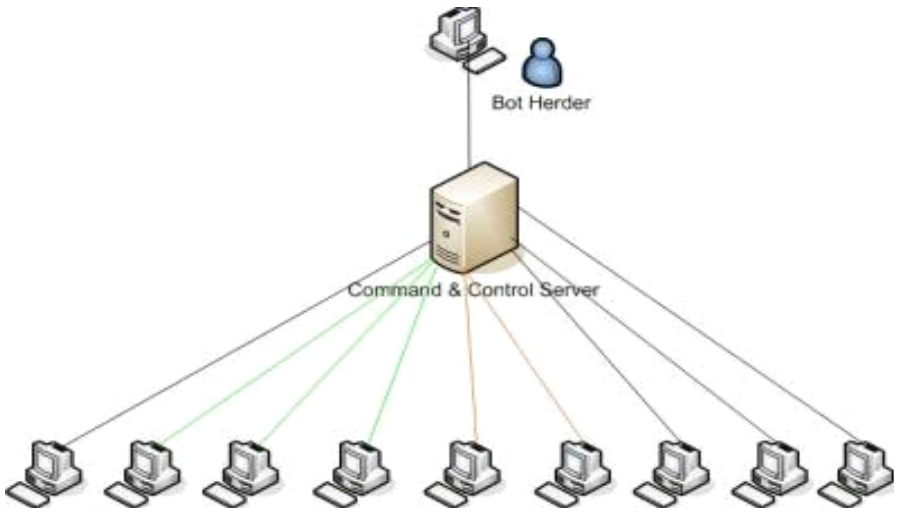


Figure 9.BotNet - Robot Network

(Source: http://bartblaze.blogspot.gr/2010/10/botnet-wars-q.html)

Usually a number of people are working together to form a botnet. So a botmaster is consisted of three parts. Someone must be responsible for the generation of bots (botworker), hence responsible for infecting the users' computers without their knowledge. Someone must be responsible for updating those social zombies (botupdater) and a C&C machine which has a database with all the commands. It is responsible to send the commands through a C&C channel and to manage the bots.

2.2.1 Bots Categories and Types

Depending on the network infrastructure (Centralized, Decentralized, Distributed), the bots either are linked or act independently. Nevertheless, they are used for various purposes on the Internet, not necessarily for malicious purposes, such as the "Trading Bots" which are used on eBay for finding the best deals in order to buy products. Concerning the malicious bots are divided into a number of categories according to their use and purposes, those are:

1. **Hacker Bots**. Those are bots that seek to exploit security holes and defects to launch attacks against user computers.
2. **Spybots or Data Mining Bots**. These are bots that collect user information and sell this information to marketing companies.
3. **DDos Bots**. These are bots that launch denial of service (DOS) attacks on webpages and networks.
4. **Chat Bots**. These bots are either used for good purposes such as answer frequently asked questions (FAQs) or for bad purposes in Social Networking Webpages by using Social Engineering.
5. **Spam Bots**. These are bots that generate web advertisements and put them on webpages, or generate bad links.
6. **Downloader Bots**. These bots download software or even complete webpages via infected computer link.

The purpose of a bot is not necessarily bad, although a big amount of bots are used for such purposes.

2.2.2 Bot threads and attacks

The most common use of bots is to use the social network of the computer user and to install malicious software in the computer. This software has the purpose of creating problems to the user or to collect information which then is used for hacker purposes. The last years many users of botnets send in everyday basis a huge amount of undesirable e-mail. These e-mails are sent through botnets and their purpose is to transmit malware as well as to steal personal data of the users (phising). By managing botnets through some methods known as click fraud, DDoS attacks, keylogging and distributing warez it can be created a thriving economic enterprise. So the ways in which the threat may be practiced are:

1. **Distributed Denial of service (DDoS)** attack. This attack type has the result of a malfunction to an operating system or even denial of services for the nominal user. The computer is at the crackers hands for future use. The denial can be temporal or even permanent in some cases.

2. **Phising** of information. This type of attack has the purpose of acquiring the identity or information about the computer user such as identity card, address information, age information, username & password of a user subscription, credit card number and bank details. During this process the attacker acts as a reliable person through his contact with the victim, in order to obtain all the information that it was mentioned above.

3. **Pharming**. Identity theft via browser with faulty webpages, identical to the original ones.

4. **Keylogging**. Software which is installed in computer that monitors and logs information about keyboard keystroke by the user so as to acquire information mainly about user account passwords.

5. **Click fraud**. There are web advertisements paid with every user click, so click fraud can be used so as to be paid with faulty payments due to random clicking.

6. **Distributing Warez**. Distribution of projects without owners' authorization or payment of fees. This is violation of the copyright laws.

7. **Stalking**. Collection of user data most of the times personal, with the purpose of spying on the user and cause problems to him/her.

8. **Scam**. This is an in-person attack through the Geolocation services, by attaining the user's location, so as to cause a physical theft of money or properties of the user.

9. **Identity theft**. Collecting user's personal data and information for the purpose of fraud, theft or charging of credit cards, bank accounts and so on. Identity theft is usually committed through e-mails which seem real from banks or from potential employers who ask the user for his personal details.

10. **Man-in-the Middle (MITM)** attack. Interruption of the communication of two or more computer users by stilling or corrupting information before the retrieval from the end user. An example is that the e Department of Telecommunications in Syria launched an attack "man-in-the-middle" against the secure HTTPS version of Facebook, as it is known that in these countries the communication between insurgents and non-citizens is through online social networks.

11. **Malware**. This is malicious software installation sending through e-mail with the purpose of stealing information, connection to a bank account or the generation of a botnet.

12. **Rootkit**. Software which is embedded into the main operating system files with the purpose of acquisition administration privileges. It lies through various images in the user's profile and when clicking on them it is installed directly on the user.

13. **Advanced Persistent Threads (APTs)**. These are persistent attacks to nations or big organizations. These attacks are done through social engineering and social networks by approaching the target so as to gain as much information as they can.

To this point it is worth to mention an important research which was done at the University of Columbia in November 2011. It was also published with the title "The social netbot: When bots socialize for fame and money" [1]. The group created 102 social bots which created their own Facebook accounts. Firstly, these bots sent friend requests to 5053 random users and 976 of them accepted the request. At the second stage of the research the bots sent 3157 friend requests to friends of the 976 users who accepted before. The results were that 2079 of them accepted the request. In 8 weeks bots had collected 14500 home addresses and 46500 e-mail addresses. This information was 250 GB. In order to be unnoticed by Facebook, bots sent every day 25 friend requests and Facebook Immune System managed at last to identify only 20% of all.

2.3 ATTACKERS

The attack on the social networking webpages and user computers takes place usually by people of certain profile, knowledge and personality and for particular reasons. The reason is mainly profit, but also personal prestige is also a motivation by some people.

The attackers have excellent computer and web technology knowledge and skills, there good in programming and sometimes even knowledgeable on the hardware. There are authorized webpage users that superset their rightful privileges with extra privileges that they are not suppose to have.

They can be divided into the following categories:

1. **Hackers**. "Hackers", known also as "Whitehats", are these attackers whose aim is either to broaden their knowledge about the mode of operating systems or software or to identify security holes or any other defects in them. Then they inform those who are directly connected with it such as the users or the manufacturers, so the problem to be directly solved. However there is a bad impression from most people about this term because hackers most of the times have good purposes.

2. **Crackers**. On the contrary crackers or **Blackhats** have bad purposes. They use the same means and methodology with hackers, but with different purpose. They like to cause problems to the computer systems in order to disable their function or even better to harm the users.

Figure 10.Hackers (Whitehats) vs. Crackers (Blackhats)

(Source:http://www.seonext.co.uk/blog/seo/blackhatvswhitehatseo.html)

3. **Script Kiddy**. These attackers are early stage crackers. They launch attacks by using known methods that have already been used by crackers. Their knowledge is minimal and they try to make impression. They are interested on the result of their action and not on the way something is done.

4. **Cyberpunk**. These are a kind of combination of all of the above.

Figure 11.Cyberpunk

(Source:http://gizmodo.com/5913004/are-you-a-true-cyberpunk-consult-this-90s-guide-to-find-out)

5. **Cybercriminal**. These are attackers who use the Internet against other nominal users. Their purpose is the profit by accessing to personal data of other users with malicious ways and means.

Figure 12.Cybercriminal

(Source:http://www.v3.co.uk/v3-uk/news/2188527/cyber-crooks-sentences-british-court-spyeye-campaign)

In addition to all above categories, there are other categories of attackers which less common and less known such us “cyber warriors", "cyber spies" and "cyber extortionists". Some of the above categories that they mentioned are also divided into subcategories, depending on the motivation of attackers.

2.3.1 Attacker’s profile

As it is mentioned from researches the attackers’ profile on the Internet it is quite difficult to be determined. Many of these persons are quite intelligent and they have spent most of their time in their adolescence in front of a computer. So another characteristic of them is that they are antisocial. Now it has proved that anyone can be an attacker. In a survey of 200 known hackers, it was reported that 90% were male, aged 16-19 years, with most of them living in the USA. Moreover, these people spend

57 hours a week on average in front of their computer and 98% they believe that they cannot be identified and arrested.

Some of the basic features of the attackers are:

1. They have good programming skills. They know C, C++ and Perl. These are programming languages and Hackers use them so as to build their tools and their applications.
2. They know how the Internet works very well and also the TCP / IP protocol to which is based on.
3. They are familiar with at least two operating systems. One of them is the UNIX. They choose operating systems which have low cost but with many tools because Hackers need them.
4. They collect computer software or hardware which is no longer used because it is considered outdated.

2.3.2 Hacker's motivations

The motivations of the hackers are many and vary depending on who is the person who does the attacks, how dangerous he is and what is the profit from the attacks. So the motivations are:

1. Economic Profits. The most obvious motivation is the profit. It can be individual or collective. In the first case, this can occur by stealing user's ID and various personal data and for access to bank accounts or by depositing money in an account after receiving a spam message. In the second case, a company may earn money through Social Engineering by gaining access to files of a competitive company purpose in order to spy it or cause problems.
2. Curiosity. As it was mentioned above there are many kinds of attackers and one of them is the Script Kiddy who launches attacks in order to see the consequences of them and more often to gain access to personal data and passwords just for fun.

3. Prestige. Hackers try to find vulnerabilities to well-secured networks and penetrate them so to feel proud of their achievement, which perhaps makes them known to the wider society and may be recruited by a network company.

4. Venom. Sometimes the attackers act by having specific targets and driven by negative emotions for their target in order to cause problems. The attacks can be addressed either to only one person or too many members of a company.

2.4 FAKE USER ACCOUNTS

The creation of a new user account on a social media, such as Facebook, LinkedIn, Twitter, MySpace and other is a very simple and legitimate procedure. It can be done from anybody without any legitimate issues.

The fact that an account is being created is not actually testing the correctness of user identification. Thus user verification is very naive and cannot be trusted. This resulted in a big creation of user accounts in the social media by bots.

When a person is creating an account, is being prompt to provide true identification and is being informed that collecting vital user information from other social network users is prohibited. This process hardly prevents malicious users from providing faulty identification as well as attempting to collect other users' data.

Unfortunately, many social media users accept friend requests, chat and exchange information with people that they do not know, without properly checking their details in a strictly caution way. In the case that the accounts of non-existent individuals are created manually and not by bots, are carefully designed with lifelike figures and are easily fooled by other Internet users or even companies with devastating consequences for them. However, the immune system of Facebook blocks strange things like that, so as to prevent as much as possible creations of such accounts.

Fake accounts though can be identified by certain characteristics, but we have to observe them very carefully I order to recognize them. After a research in many fake accounts we found some specific characteristics, which are:

1. Non correspondence between name and profile photograph
2. Many repost from advertisements or from applications such as TwitterFeed from Twitter. The user can install this application so he can have all the daily news posted to his profile for example from CNN.
3. Unanswered comments on user's wall from other users like "Thanks for the add".
4. Repetition of the same answer to comments.
5. Spelling mistakes.
6. Friends from many different countries.

7. Postage of many spam messages.
8. Strange information such as corner value date of birth (e.g. 01/01 or 31/12).
9. Activated the auto follow option.
10. Profiles of famous people with misspelled name.
11. Usage of tinyurl in a status.
12. Small number of @replies on Twitter.
13. Having much more Following than Followers on Twitter.
14. Use Default Security Settings.

Continuing we will see some examples of attacks in the social networking websites.

2.4.1 Spam Messages

One of the common ways that intruders choose to annoy authorized internet user is to send a massive amount of spam messages. Those messages are mostly infected and sometimes are not even legitimate.

Figure 13.Spam Messages

(Source:http://www.pc1news.com/news/0107/india-generates-least-spams-among-bric-countries.html)

Spam messages are design so as to attract users' attention and interest to 'click and find out'. But once they are read by the user they install in the computer infected software. Those people who send these messages are called spammers. The senders of spam focus on the presentation of their messages. They use glorious titles and the content of their messages is mainly constructed in HTML. However, they use text in simple form so as to bypass spam filters. Spammers take care to be aware of current events, but also for the interests and preferences of the user, so the messages they send to be plausible. The request to add Dislike Button on Facebook, various rumors about the photos of the dead Osama Bin Laden, the advertisement of the next movie "Twilight" and various supposed revelations about famous persons are used as themes in "mask" attacks by dishonest individuals for promotion of infected software and theft users' identity. Although social engineering messages give the impression to users that come from secure and trusted sources. Spam messages that daily circulate in SocNets can be distinguished in the following categories depending on the format of the message and the purpose that seems to have their senders:

• Spam messages with attachments

These messages are intended either to the collection of addresses and other personal data of the users or to the transformation of computers into bots, through the installation of malicious programs. For example, in 2010, 2 worms and 1 Trojan program proved very popular among the most popular spam sender SocNets.

• Economics spam

This kind of spam aims to steal money from users. Many users have received messages from friends (their account is broken) in need, asking for money. Two years ago another sample message appeared in social networking sites which informed the user that it has detected malware on his computer. He could be relieved from this through an antivirus product from a known company with malware programs named FraudLoad.

• The Nigerian letter or "419"

The name comes from the violation of Article 419 of the Nigerian Criminal Code. The spam displays the sender, the user of the social networking service as an officer of the Nigerian government or a retired government official, usually speaking for a rich died man who offers to the recipient the "opportunity" to share a percentage of his fortune. But he asks for help in the payment of taxes, with the promise that all expenses will be returned once the funds leave the country. This is all completely false and the sender is just trying to divert money from the recipient, asking him to send personal data such as bank account number and so on.

• Promotional spam

This type of message is only used to promote products or websites, without any further illegal profit. Sometimes the senders use titles with different content of this in the website in order to attract as many users as they can.

• Chain letters

This kind of spam messages use phrases like “Send this message to 10 friends and you will earn .. “ and in this way they can obtain data from the sender. Then they will use these data for malicious purposes.

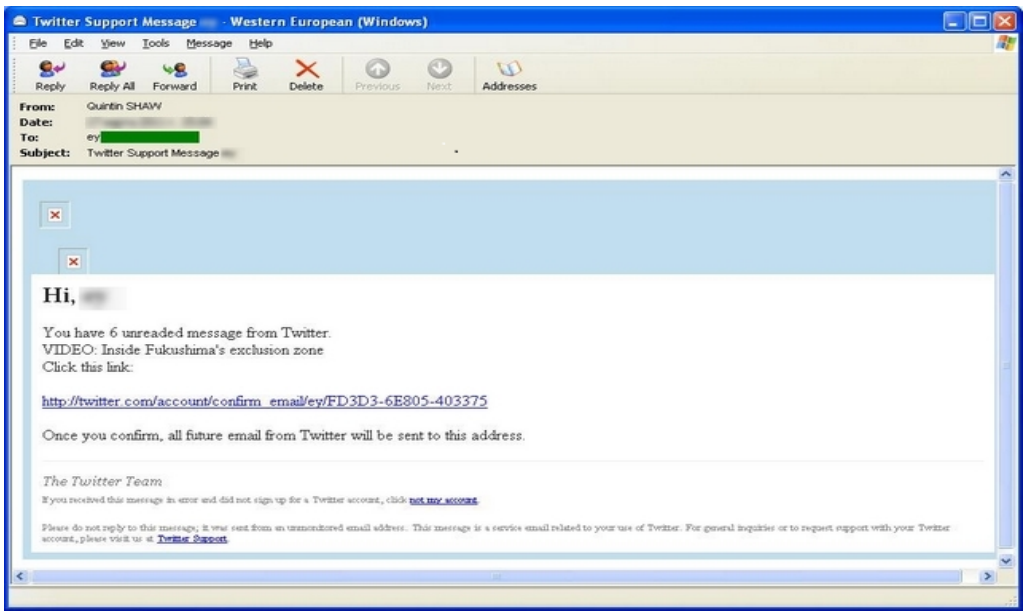


Figure 14.Spam Message

(Source:http://www.securelist.com/en/blog/6123/Japan_Quake_Spam_leads_to_Malware_Part_3)

• Spam messages sent by the supposed management team of the websites

These spam messages are sent to users' e-mails from the social media and they are presented as administrators of the services. The layout of the message automatically copies the web so that it is plausible and convincing to the users. The purpose of these is the promotion or obtaining personal information from users. An example of this happened on Facebook when a message was sent among the users supposed that it was sent by the management team of the service. This message invited the users to confirm their account via a link in order to get rid of the spam messages. If the user selected the link the spam message automatically was sent to his friends by spreading a malicious code. A similar message like that is the message named "Facebook password reset confirmation".

2.4.2 Viruses & Worms

The number one goal of manufacturers viruses have become the social networking sites. Facebook has received many attacks from its very beginning until today. Some of these attacks were perceived by their users because of their obvious consequences, but users ignore most of them. According to a survey conducted in November 2010 by a company named BitDefender, 20% of posts of Facebook users hide threats, 22% of those claim that they will notify the user if, for example, the user has been deleted from another user or how many users see his profile every day, 15% offer gifts for various games such as Farmville, and 11% advertise the integration of the option "dislike".

So we understand that viruses are not only in various applications of social networking websites, but are also hidden in messages and publications even though in chatting. Nonetheless, the victims of these attacks are not limited to users' computers. These malicious attacks also affect the dignity of users without knowing it. Many times these viruses are spread to all the users' friends through messaging.

One of the most known viruses that hit the social networking sites is the virus "Koobface" which first appeared on Facebook in 2008. A few months later, this virus was made again a comeback, but in another form, transforming the user's computer to bot. The management team of Facebook directly published instructions on how to remove the users this

virus from their computer, those who were infected. Nevertheless, the "campaign" virus Koobface did not stop there. In late 2009, they began again to spread the virus through publications or messages containing links of video which provoked the curiosity of the user such as "I can't fall asleep after viewing this video; I haven't seen anything like this before ". Right now, there are more than 4,000 versions of the virus Koobface, as the creators of the virus constantly revived it in order to avoid its detection and to continue their work.

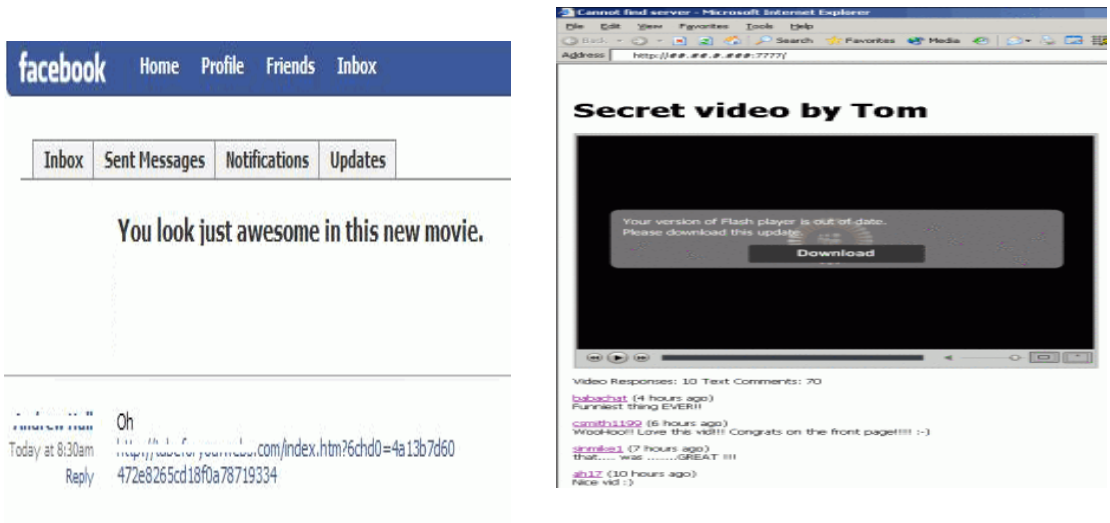


Figure 15.Virus Koobface

(Source: http://news.cnet.com/koobface-virus-hits-facebook/)

One the most serious viruses circulating in SocNets is the Ramnit. According to reports, the virus first made its appearance in April 2010 and it is estimated that it is responsible for 17% of total Internet attacks worldwide. It is mainly used for interception of data related to bank accounts and credit cards and it was spread through links that lead to infected websites. More than 45,000 are the victims only on Facebook of this malicious software.

The term "Cross-Site Scripting" refers to a type of applications which allows attackers to bypassing security mechanisms provided to users through web browsers that they use. They insert a malicious script and they gain access to sensitive page content maintained by the browser for the user.

2.4.3 Third Party Threats

The various applications on social networking sites have become a favorite habit in everyday life of most users. On Facebook, specifically, which gave for the first time in 2007 the ability to create different applications to users and developers, it is rumored that there are now more than 15,000 apps. Applications, such as games, various quizzes, daily updates, calendars and many other apps cause curiosity and interest of the user. But who is behind these applications? Almost all applications created by third parties and not the management team of Facebook. So if someone wants to install an application, he needs to give all his personal data to the creators. Many users do not care about that and they do not think the consequences and they give their data.

In a research conducted by the University of Virginia it was found that only 8.7% of total applications did not require access to the user's personal information, 82% of them saw as many data as the user chooses to show publicly and the remaining 9.3 % needed all the private personal information. However, according to an article published in the Wall Street Journal, many of the applications on Facebook sell personal data of users to research companies and advertisers. The management team of Facebook of course asks from developers that the users' data not be used in a malicious manner, something that cannot be confirmed.

Mafia Wars, Farmville, Zynga Poker, Restaurant City are four of the most popular games on Facebook. More than 63 million people play Farmville every day. Unfortunately there are applications in four games related to financial frauds. Specifically, Farmville enables the user to create their own virtual farm with some virtual money offered by the application, but the user has to spend so much time. If the user wants to speed up the whole process and to acquire other goods, he can invest real money, either by credit card or via PayPal. Users have also the possibility to acquire virtual money by accepting some of the deals that make various advertisers around the game, like to be subscribed to some websites that provide a credit card or even to take an IQ test by giving the cell phone number. In the latter case, the combination of user's mobile phone and a password that will be requested is a very good trap. The user is subscribed in services by paying without knowing it. As we understand, this offer is addressed mainly to children.

The virus Profileye, in March 2009, disguised as an application on Facebook which emerges to the user which of his friends frequently visited his profile ("Someone visited your Facebook profile page. Please click here to see all your visitors") tried to gain access to notifications and to personal data of the users inviting also all friends of each user - victim to install that application. A few months earlier had made its appearance a virus similar to the Profileye which was used as a mask of an application known as "The Error Check System". This application prompted the user to install it in order to detect errors that exist in his personal page. The effects were same as above.

Quiz with a very innocent titles like "Which Disney Princess are you?", "What's your temperament?", "Who is your ideal partner?", "How long are you gonna live?", they want to see who are in real the users, making them questions about their interests, their views, their hobbies and so on. Through Social Engineering and these applications creators can easily engage in financial fraud or pinching users as online friends if they know so much about them. However, there are other more dubious quiz titles such as "What does your password say about you?", where the creators real aim wants to say "Is your password easily going to be hacked or is it ok?". According to surveys, there are more than 800 people who have responded to such online questionnaires.

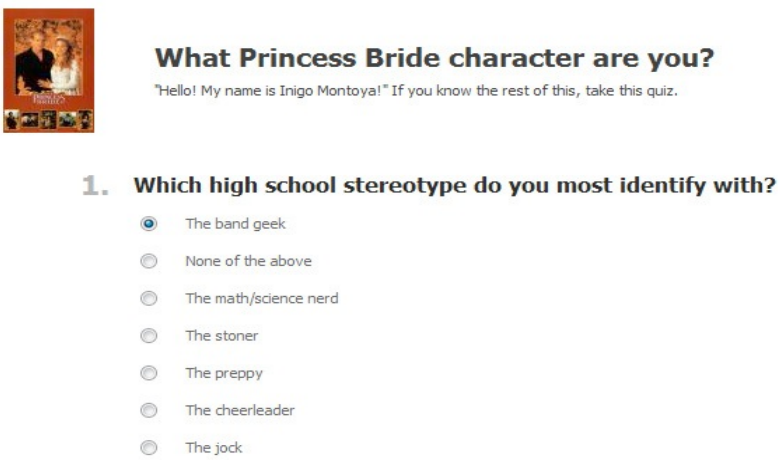


Figure 16.Quiz on Facebook

Recently was discovered by some researchers of Symantec that there is another fake application which steals the login information of users on Facebook. It displays an error message when you view a video, in which the user is asked to reconnect in order to continue. This leads him to a seemingly same page with Facebook (but the URL is fraud) and in this way it steals the username and the password. The AVG Company reveals that there are up to 9.700 applications which are vulnerable.

Using applications to connect in internet via mobile phones leads to new kind of attacks. Many applications have been found and identified as malicious but the most known is FaceNiff. This application made for Android phones, enables users to connect to their Facebook account, Twitter account or YouTube simply connected to the same network of the holder of the application, even if this network is protected with encoding. Now we have to wait what will happen in future.

2.4.4 Advertisements and Links

The virus writers try to find different ways to infiltrate to the users' computers, so except of applications and they also use advertising, exploit the curiosity and the consumers' habits. In this case one of user's friends publishes to his profile an advertisement or a product in which are commonly used phrases such as "He saved my life!" Or "The best I've used up now" so as to motivate the user-victim to get to those links. So the viruses behind the advertisements usually lead to multiple posts of the same ad to friends of the user who just became infected.

Another widely used attack technique is one that involves the use of limited address. This attack mainly unleashes through a fake account where the attacker publishes a link to a malicious website which is quickly spread to all his friends. The user cannot understand if there is some danger behind a shortened URL so it follows it from curiosity because his friends do it. According to studies from Symantec in 2010, 65% of the malicious link published in the newsfeed of users who use specific addresses and the 33% of them has been selected by 11-50 users.

The term "Cross-site request forgery" is used to describe a type of attack known as "one-click attack" concerning the malicious use of a website where taking advantage of the rights of an unsuspecting user we can execute unauthorized commands via the browser and via the stored cookies. In this kind of attack the attackers tempt the unsuspecting user through a publication in the profile of a friend. The user-victim visits the web page which can contain a special code JavaScript. This code triggers a series of processes that generate false consent of the user to every social networking site is connected and publishes a link that leads to an infected website without even the user being aware of. This kind of attack based on the vulnerability of social networking websites and how to authenticate users for each activity as they rely on stored cookies from browsers without checking the source of the changes that required to occur at specific accounts. As far as Facebook concerned the administrators informed users that there is an automated system that deletes posts with suspicious links from profiles that may have been violated and then ask from their holders to change their password in the service.

Another way of attack is through "Clickjacking". The attacker can trick users from a social networking website urging them to visit seemingly innocent websites in order to reveal confidential information from them and then to take control of their account or of their computers. This kind of attacks have occurred on Facebook, for example, exploiting the feature "like" of the service through publications in the profiles of users, spreading in this way a website with enticing content as bait. If a user visits this site he will be asked to press a button by adding automatically in this way this link in his profile. Experts in security note that this kind of attacks do not carry so far infected software or do not lead to attacks phising but maybe in the future may be used for these purposes.

2.4.5 Social Engineering

Social Engineering could be described the "art" which used by attackers for indirect attack on the system. It targets the most vulnerable security factor, human. The steps so as to achieve this type of attack are:

1. Find the target

In the first stage of the attack, the attacker gathers information about the system in which he wants to attack, as well as data of users who have access to it. The attacker in order to find the data uses search engines, social networks, metadata and various tools to create the profile of the target so as to find a way to approach him without being noticed. This stage is based mainly on the Open Source Intelligence (OSINT) which finds the available information, analyze and use it. We have some examples of these tools:

- Search Engines for Social Networking Websites

On the Internet there are over 20 search engines to social networks, such as the "http://www.whostalkin.com/". The only "disadvantage" is that it can detect only those users that are publicly available. There are also machines that seek data on networks like YouTube or Flickr.

- Maltego

Maltego is an open source application, which is supported by all major operating systems and is also provided by the Backtrack. Maltego has also a library of different transformations to find data from open sources on the Internet and enables the collection and display of this information in a chart suitable for data mining and analyzing real relationship between humans and the correlation of these with profiles on social networking sites, websites and networks. It is considered one of the best tools that can be used for this purpose. It has a perfect “fit” on Twitter as it can detect

even talks but as for Facebook the access on it stopped for now due to a change in the code of the platform.

- Google Doks

As we know, Google's search engine is the one most used by Internet users, because of the accuracy of the results that it gives. Google has some bots, which control all over the Internet and copy web contents in company's databases. For achieving greater accuracy in the results of search engine, Google uses some words, known as dorks. These words can be used for a good cause but also for malicious purpose because as we mentioned above the bots store usernames, passwords, and so on. So they can be used in our case in social media sites for information extraction.

2. Attack

At this stage, the attacker approaches the victim-target through social networks trying to win his confidence and using various methods, accomplishes his purposes. Based on Social Engineering we had already several attacks on social networks with the most prominent of all the known fraud "I'm stuck in London" which took place through Facebook Chat. With no cost the attacker used a simple profile on the network in order to obtain money by the following conversation with the user - victim:

"Attacker: hi what's up?

Victim: hi Matt. Everything ok?

Attacker: well I am really stuck here in London. I had to visit a resort here in London and I got robbed at the hotel I am staying. "

This solution is then followed by other malicious users who created ChatBots to automate the process and led victims to dangerous websites or applications. Attacks like them can be conveniently studied by using the Social-Engineering Toolkit for research purposes. This is an open source tool for testing various types of attacks which is provided by the Backtrack.

Finally, for the successful implementation of these types of attacks it must be developed a plan in order to be faithfully followed so as to lead the attacker to reveal the desired information from the user. There have been several studies on this subject and the most recently was contacted by a research group in Austria [2]. The group presented the "circle of delusion" which was based on the performance of an application with an automated Social Engineering attack by using ChatBot on Facebook. This "circle" described all the steps which are involved in this attack.

2.5 SOCIAL NETWORKING WEBSITE ERRORS

As we said before the social networking websites and the way that they operate, contribute to the lack of privacy and security. A typical example is Facebook, which, according to Emil Protalinski (2011, source: http://www.zdnet.com/blog/facebook/three-weeks-later-facebook-has-paid-40000-in-security-bug-bounties/3115) who gave $ 500 pay to any developer who was able to find security weakness. In 3 weeks, Facebook paid a total of $ 40,000 for discovered failings and for the most serious of all to be priced at $ 5,000.

However the mistakes do not stop at the security failings. As far as Facebook for instance is upgraded, its security to users is decreased. In its new version, there are two options for a friend request, the "Accept" and the option "Not now". If the user chooses the latter, he has not denied the friend request, but he has essentially put it on hold. This option still allows the other user to have access to the basics of personal information of the others, something which most users are unaware of.

There is also a mistake in this matter from Twitter which does not protect its users completely. The choice "autofollow" on Twitter handles the requests from other users. By having someone a friend request from someone else, if activates this option, automatically accepts - "follow."

Another "innovation" of Facebook was the change in the security settings, by using the default option so all user data to be public and every user has access to them regardless of the existence of friendship. Some time ago it was published on the Internet that that the operators of Facebook allowed to some developers to have access to phone numbers and addresses of users, something which is temporarily suspended, after users' complaints. The account creation process, with the absence of course of a certification, to those pages is another element that makes them unsafe. Aside from the obvious mistakes there are some other errors in the service by searching it, such us the easy access in any account on Facebook, by selecting the "Forgot your password?". There is in the log in form and if you follow the specific steps, they lead you to the addition of an alternative account e-mail.

Subsequently in 2011 Facebook made major changes to the design of its web pages by adding some “operating systems”. One of them was Ticker which is on the right column of the homepage of each user and displays in real-time all user activities. As it is obvious that this is another element that shows us that safeguarding the privacy of users is not on the priorities of the management team of Facebook.

Users also can store to their computers personal photos of their friends as now provided the option "download" under each photo. Finally, one of the latest shocking findings was the addition of a new status update about having a child. The future parents will be able to inform their friends about even the probable date of birth and the worst of all is that without the parental consent, it is constructed a profile of their child, which is added to their family members.

However, the creator of Facebook, Mark Zuckerberg, says that users do not need security and privacy. So how is it possible the terms of service and the privacy settings to ensure the users’ protection of the most popular Social Network?

Now on Twitter and Facebook has incorporated a new Geolocation platform called Foursquare, through which users can at any time say their geographical position on the map, informing their friends where they are and with whom. This new feature of the social networking service is particularly dangerous as everyone knows when someone is missing from his home which is also especially challenging for robbers who can be hidden behind a fake account. It is worth to be mentioned that two Dutch developers who wanted to show the dangerousness of this service, constructed a Web page via HTML and JavaScript which called "Please Rob Me".

Figure 17.Please Rob Me

(Source:http://laughingsquid.com/please-rob-me-a-website-listing-updates-from-people-saying-they-are-not-home/)

This service was seeking and displayed in real-time all the house addresses which were declared from Twitter users and as a result was to collect hundreds of them. The location-based services are predominantly used in smartphones, where through the GPS, is recorded any time the geographical location of the customer which is unknowingly kept in a history. In fact, this service is now so popular that it is estimated that now its earnings will exceed $ 1.3 billion. Therefore, the more users use it, the more attackers will turn to this application for launching new attacks.

2.6 COMPUTER SECURITY/CONTROL

The social networking sites based on human relationships and communication, encouraging their users to post more and more personal information to them. A direct consequence of the above is to consider the social networking websites as a goldmine for launching social engineering attacks by cybercriminals.

As users of Facebook and Twitter numbering in the hundreds of millions, it is logical that these 2 websites are ranked at the top in the list of prospective rogue. The messages which are traded among users are so many or even posts that contain links that hide an infection. Once the user enters to them the computer turns automatically into a zombie and then the existing zombie network sends to all friends the same message. In case a user's computer turned into a zombie, he/she might not lose data, but generally his computer will delay every time it connects to the Internet. Unfortunately, this kind of infections are difficult to be observed and deleted as most of the times their files bearing names similar to those system files. According to published research based on Twitter, 24% of tweets which are daily published, come from bots and reach the number of 150 tweets per day.

So as social networking sites are booming and are gaining more and more users, it is very important to provide them protection, either through their education or through those sites. In this way they avoid as much as possible attacks and their impacts and the most important they ensure the security of their data.

Initially, the training of the users of social networking sites can contribute significantly to their protection. There is a website on the Internet named "SocialMediaSecurity.com" which provides a free guide with the name "Facebook Privacy & Security Guide". This guide is updated with any changes are made on Facebook and helps the users to set correctly the security settings of their account. Besides that the users should be informed on how to recognize fake profiles, spam messages and viruses. Informing users could be done in several ways, such as through leaflets, broadcasts and even through the social networking websites providing, for example, an interactive way to inform via a video or via notifications concerning risks which can be identified.

However, a major role in dealing with the “Social Malware” plays the browser which according to the «PC Magazine» the safest Explorer of all is the Internet Explorer 9. Specifically, in a study in the "NSS Labs" that the Internet Explorer 9 the 99.2% of links with malicious websites. It uses a technology named "Application Reputation" which evaluates the various applications. It is also worth mentioning the respective percentages of other browsers. The second safest is the "Chrome", which blocks just 13.2% of these cases while in the third place with 7.4 % we have the "Firefox 4" and "Safari 5".

Facebook integrate new methods of security by controlling the connections on it in order to protect its hundreds of millions users. To be more specific, the user can choose, from the new security settings, to receive an e-mail each time he or someone else connects to his account through a device that has not been used in the past. In this way he can check whether there is a suspicious move on his account and when exactly was the last connection. Moreover, if, for example, there is a simultaneous connection of 2 different points into one account, Facebook act immediately, without notifying the first user.

In January 2011 Facebook introduced two new features that ensured the safety of users and specific the "secure connection" and the "social captcha". Specifically, in "secure connection" on Facebook, HTTPS has been applied which refers to the combination of the HTTP protocol and the protocol SSL (Secure Sockets Layer). HTTPS protocol provides the ability to encrypt data traveling between the servers and the user, so data cannot be intercepted by others or infected software or through "man-in-the-middle" attacks. This method is recommended for users who are often connected through free WiFi networks. If a user wants to activate it, he should choose from the account settings the "Security" option and then to select the "Secure Browsing". On the second security method we can say that it is related to the immediate incident response when an incident is mentioned suspicious by Facebook. For instance, we can have a simultaneous connection to an account from two different locations on the planet. Specifically, the user is asked to recognize some randomly selected friends through pictures so as to be identified if he is the real owner of the account. However, this feature has not appeared yet to all users of Facebook. Apparently, Service managers want to give the complete profile control to users in order to pacify organizations which are in favor of the personal data protection.

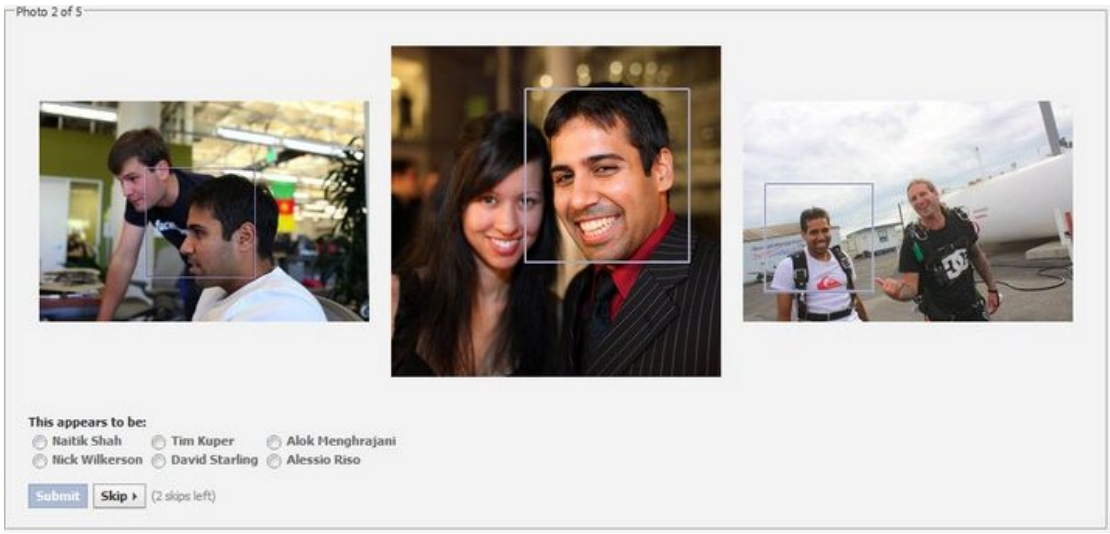


Figure 18.Social Captcha

(Source:http://www.almostlikeeverything.com/facebook/facebook-https-social-authentication-captcha-security/)

A few months later Twitter followed the steps of Facebook and applied the secure connection by using the HTTPS. Specifically, users of Twitter can now choose from the security settings the option "Always use HTTPS" and they can connect in their account from any computer or mobile phone and network safer.

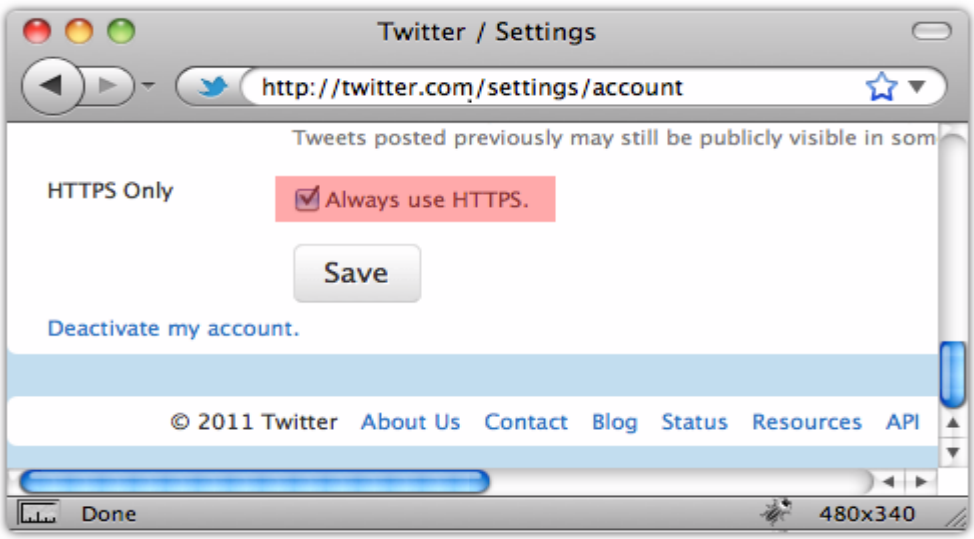


Figure 19.Use of HTTPS on Twitter

(Source:http://nakedsecurity.sophos.com/2011/03/16/twitter-goes-secure-goodbye-firesheep/)

Twitter also has integrated a service responsible for automatic shortening of links. But this service controls the link that is shared by the user so as to avoid as much as is possible phising attacks.

We should also mention that Facebook has a page which provides advice on the users' safety and give information of any new kind of threat that appears, so to know users what can do if their account has been compromised. Similarly, Twitter has a blog to inform its users for any news and dangers.

The managers of social networking websites must provide to their users safety. So they have to control the developers of the applications and to be strict when they give access to resources related to the system. In addition, they should check the already made applications before they are available to the general public.

Continuing we have advices to users for a safe use of services like Twitter and Facebook:

1. We choose to hide the email address from our profile in order to avoid spam messages as many are the spammers who use tools known as "Harvesting Bots". These tools record the email found on websites and with combination of other personal data, lead to economic frauds. We can also have an additional infrequently used, email address so as to get subscribed on such websites.
2. To be sure that any information posted on our profile cannot be used to verify our identity.
3. We activate the security question in our account, so if it is stolen we can easily retrieve it by confirming our identity.
4. The complexity method helps to remedy the violation of the codes access. So we use different password from those that we may have to a site which is most important to us and we make sure not being so simple.
5. We should not post to these services a lot of our personal items as we do not know how they can be used in the future. Even if we delete them, they are still stored on servers. We have to check regularly the privacy settings because they change frequent.
6. We have to be very careful when we accept a new friend on these services especially if we do not know him.

7. In many social networking services provided the opportunity of the separation of the user's friends so as to control the access to his personal information.
8. We never give to anyone our personal data. The company VeriSign provides to the Internet users at the website "https://www.phish-no-phish.com/", a questionnaire and the users can test their skills in recognizing phising websites and get informed about them.
9. It is better to do log out each time we want to leave a site in order to delete the session cookies.
10. We never respond to spam messages and do not visit links that may contain, even if they come from friends. In this case, we inform our friends that we have received one of these messages from their account.
11. We do not send spam mails to friends.
12. We pay attention to the messages that our friends ask for our financial support and do not believe them.
13. We do not be affected by messages with titles like "earn easy money" and we should immediately delete them.
14. Facebook has an application named "Norton Safe Web" by Symantec, which controls the feeds of the last 24 hours and informs the user about the links which are considered safe, dangerous and untested.
15. If we want to do a financial transaction over the Internet, it is to use another browser from that we are connected.
16. We are very careful with those links which imitate the website of Facebook and we check their URL.
17. We do not publish all the time where we are by using Geolocation services like Foursquare.
18. We avoid links that have been published by many of our friends and links which links which contain phrases like "funniest ever".
19. We do not respond to applications which ask our personal data.
20. We allow access to third-party applications only if we are sure that it is safe, by checking the developers and reading reviews of other users. However, if we do not want an application we can delete it from the settings of our account.
21. We should avoid the connection to these services through public wireless networks.
22. Before we do an action on the Internet, we have to check for suspicious signs and also not to trust pompous titles.
23. We do not forget that at any time we can be victims on the Internet. It is known that we have on average 55,000 new types of attacks every day.

24. If we fall victims of a fraud, we inform through a publication our friends and we change in any case our password. We also mention the fraud to the administrators of the service.
25. We have installed in our computer an up-to-date security software in order to protect it from viruses and infected programs.
26. We schedule at least once a week a full check of our computer files, then we defragment the hard disk and we clean the registry memory through special programs. It is also advisable to clean the temporal memory or all browsers on our computer such as History, Temporary Files, and Cookies and to keep it updated.
27. There are many free tools on the Internet which can help us to check whether a website that we want to visit is safe.

It is widely known that the risks for kids are great. It would be good the school to give at children some information about the advantages resulting from the proper use of the Internet and the risks that are involved. It would be also wise, parents to prohibit from their children the access to certain internet sites as long as they are very young by using a software filter.

As far as the companies concerned, they could use technologies but also to follow certain procedures in order to ensure the safety of their data. They should be aware of the value their information systems and to learn about potential threats from their qualified staff.

To be more specific:

1. Use of software known as Sandboxes for the control of the files and programs without the fear of bad consequences.
2. Use of Honeypot technology in order to create an environment that is an imitation of the real. With that way the attacker is attracted and trapped in a virtual environment in order to immediately be identified his presence and be analyzed his behavior.
3. Use of a monitoring traffic network and an incident recording file.

2.6.1 Ariadne program

In the field of security on the Internet it is worth to be mentioned the program “Ariadne” and the useful services that offer. Ariadne is a Training Program on mental health and it has to do about the phenomenon of the adolescents’ "addiction" on the Internet and the dangers that children face from the uncontrolled Internet usage. This program is working in co-operation with the University of Athens and a Special Account for Research Grants through the Adolescent Health Unit of the Second Pediatric Clinic of the University of Athens and the Training Centre “Ε.Κ.Π.Α”.

Ariadre tries to protect children, adolescents and their parents from the dangers on the Internet by informing them and supporting them in every question and problem occurs.

The most significant problems that this organization focuses on are:

1. Reliability of context on the Internet and especially on social media.
2. Publication of personal data on the Internet and reporting emotional states.
3. Grooming
4. Identity theft or codes’ theft.
5. The phenomenon of cyber bulling.
6. Games on the Internet and on Facebook.
7. Excessive occupation with the Internet.

Are the social media and the Internet blessing or curse? Social networks have redefined the way that million children and adolescents communicate worldwide. But, do they spend more time than they should?

Figure 20.Usage statistics on Facebook

(Source: http://www.tanea.gr/news/greece/article/4683730/?iid=2)

In Greece children enter in the world of Facebook ... from kindergarten. According to recent research by the Greek Safer Internet Centre, two of ten Greek children aged 4-6 surf on the Internet from home, while 1% has its own profile in social media. In elementary school, 15% of students have an account on a social network, while in middle school and high school Facebook is very popular, with 60% of students to have created profiles on the site. We are facing a new phenomenon. If once the parents knew that their children are playing in the square, now they are on Facebook, without their parents knowing what Facebook is and what their children do in there. Moreover, in the past, parents were fighting their children because they were watching many hours of television, neglecting their schoolwork. Today, parents try to take their children off the computer because they spend many hours in online games and in social media.

We have some statistics about the Internet usage from children:

1. One with two kids of the 14% of the kindergartens in Greece has already created his own profile on Facebook.
2. One of ten infants uses the Internet out of school.
3. Five of ten kids of elementary school use the Internet in their home.
4. Two of ten kids of elementary school have Facebook profile.
5. Nine of ten students of high school use the Internet out of school.

Children in Europe use the Internet on average 88 minutes every day, on the contrary to children in Greece who use the Internet and the social media 8 hours on average every day. Many of them are addicted to social networking. They want to learn what their friends do every second and make new friends. They want to be accepted from everyone by using the social media and posting photos and everything else personal on it. Some of them they do not have real friends so they try to make Internet friends. There are kids that are really lonely even from their families. It is shocking the example from the Ariadne program where a child called and said that he uses the social media because he wants to say "goodnight" to his friends as his parents are missing all the time and he does not have someone to say "goodnight".

One of the most important dangers on the Internet in the "grooming". It usually takes place through chat rooms and through social networking pages such as Facebook, MySpace and Twitter. It describes the behavior of a web user who is intended to inspire confidence in the child so as to carry with him a secret meeting. The sexual abuse of the victim, the physical violence and abuse through pornography may be the outcome of this meeting. According to a recent survey, Kopecky 2010, 56% of grooming is through messaging services while 11.4% of cases occur through social networking services.

Figure 21.Grooming

(Source:http://psychografimata.com/11498/apoplanisi-meso-diadiktiou-grooming/)

Some solutions for the parents that Ariadne suggests are:

1. Parents should dedicate time and surf on the Internet with their children, together.
2. Parents should agree with their adolescent children on how many hours should surf on the Internet. They should not overcome 10 hours per week.
3. Updating of children about the phenomena of addiction annoyance on the Internet.
4. Using filters for malicious webpages that teenagers prefer.
5. If parents notice excessive use of the Internet and phenomena of addiction, they can ask help from organizations such as “Ariadne” and “ΥΠΟΣΤΗΡΙΖΩ”.

Figure 22.Helpline "ΥΠΟΣΤΗΡΙΖΩ"

(Source:http://www.saferinternet.gr/index.php?parentobjId=Page187)

Last but not least, we should mention some rules from the ministry of education concerning the safe use of social media specifically from the elementary schools. It is widely known that nowadays children use also the school Internet in order to have access to the social networking webpages. This is as dangerous as the use from the home because children surf on the Internet without limits. So schools also should take some measures. One of them is that the headmasters of the elementary schools can request from the Greek school network a limited timed access to the social media so as to have the control of them.

In any case teachers and students can use the safe provided Internet at school for their educational needs. Some of them are:

1. Social Networking and Blogging service for schools, teachers and students (http://blogs.sch.gr).
2. Asynchronous eLearning Service for sharing educational content (http://e-learning.sch.gr).
3. Electronic Order Service to support and improve the educational process (http://eclass.sch.gr).
4. Educational Video Sharing Service and exchange views and commentary (http://vod.sch.gr).
5. Teleconferencing Services and eLearning (http://conf.sch.gr).

For the members' information of the school community on issues relating to the safe Internet use such as educational and information material, schools and teachers may be addressed to Informative Site for Safe Internet (http://internet-safety.sch.gr) which has been created from the Ministry of Education and the Greek Safer Internet Centre (www.saferinternet.gr).

CHAPTER 3: PROBLEM DEFINITION-CONTRIBUTION

3.1 CHATBOTS

Social networking is possible for an attacker to use messaging services in order to carry out attacks without wasting much effort and time by using programs which are designed to mimic human behavior and writing so as to not be perceived by the human user. These schemes use artificial intelligence technologies that are not very smart and are generally still in its infancy. However, we can think that in 1012 Facebook serves 900 million active users and by using the ignorance of them it can realize mass attacks which are efficient in such large number of users. Attackers use Social Engineering techniques to take from their victim's valuable information, money or to install malicious software on their computers.

To be more specific, ChatBot is a computer program designed to personate an intelligent conversation with one or more human users. It first designed in order to fool the user into thinking that he has a conversation with other humans. These programs are referred as technical interactive entities. Some ChatBots use sophisticated methods for their operation but most of them are just looking the user's input into a knowledge base and get the answer by matching keywords or the most similar arrangement of words.

ChatBots currently use techniques of Social Engineering to gather information for the victims from social networking sites like Facebook before make any attack. Services for instant messaging can be used to automate these attacks. Goal of automation is to reduce the time of human intervention which is the ultimate goal of the attackers. The classic Social Engineering attacks are very expensive because of the equipment and time consuming until the social engineer can accomplish to "build" the necessary relationship before the attack. On the other hand, bots that make automatic social engineer attacks require minimal human resources in time or in cost, so such an attack is promising.

Apparently, there are many kinds of ChatBot attacks and especially from Facebook ChatBots which are the most famous and are the main topic for research in this thesis.

Two years ago it appeared a malicious app named ChatSend which was working through Facebook. It is advertised as a social file sharing service which enables its users to share files on Twitter, Facebook and Google+. In

reality this app chooses accounts from Facebook and uses them as a home base in order to send spam messages. It sends automated messages to Facebook users' friends saying that they downloaded ChatSend. It shows a URL that instantly downloads the application to user's computer. However, there is an obvious difference between the actual URL and the fake but users have to be very careful. Unfortunately, more than 136000 people have already "liked" this app on Facebook. ChatSend has been marked as a malware from the management team of Facebook and likely it was blocked.

Figure 23.ChatSend app

(Source:http://news.softpedia.com/newsImage/ChatSend-App-Abusively-Sends-Facebook-Messages-2.jpg/)

3.1.1 Available ChatBots

- MirandaIM

Miranda IM (Miranda Instant Messaging) is an open source instant messaging program and is only supported by Windows. Provides a basic framework client, a graphical user interface (GUI), supports various IM protocols such as AIM, XMPP, IRC, MSN, Yahoo and the use of various plugins, more than 500 including the AnnatheAlicebot.

We can see in more details how the AnnatheAlicebot works. AnnatheAlicebot is basically a bot of ALICE adapted to run on the chatclient MirandaIM. The personality of ALICE is entirely made of AIML files but it can be modified to make our own personality and to answer to questions that we want. There are many AIML files available online in which we can build a very clever bot with themes such as politics, history, literature, movies, music, science and so on. Hence, we could easily create an ALICE that behaves maliciously serving our own purposes without being easily perceived.

- JAXL

Jaxl is an object-oriented XMPP framework in PHP for developing real-time applications. Downloading this program we define a number of different proposals that we want to send to the user after each response. It does not incorporate artificial intelligence functions like MirandaIM but it can be used to exchange automated e-mails that will try to stimulate the interest of the user so that he can visit a website that we want. If we want to run the program we can first change the config.ini.php as follows:

```
// Set an environment

$env = "prod";

$key = array("prod"=>array("user"=>"facebook_username",

                "pass"=>"facebook_password",

                "host"=>"chat.facebook.com",

                "port"=>5222,

                "domain"=>"chat.facebook.com"
```

- Rep.licants.org

Rep.licants.org is a web service that allows users to install a bot of artificial intelligent in their Facebook account. With a number of different techniques the bot tries to emulate the behavior of the user and to improve it by making posts and creating new contacts with other users. The bot is not created with fake ID but is formed with the identity of the user that can be changed as desired. For instance, we can define at the bot the

themes that we want to publish on our Facebook account. This can be done by specifying the keywords such as digital art, philosophy, Roger Federer and so on.

Even though, the creators built it in order to allow the user to increase his popularity on Facebook, someone could use it for malicious purposes. One way would be to create several different Facebook accounts and then to install this application where it performs new friendships, automatically. Then it could attack through the techniques shown above.

As we can see in the picture below it has created a fake profile with installed application Replicants. The bot has done post on the user's wall with issues that he defined by himself. Here we have arts and tennis. Moreover, in two days, he sent to his friends a message asking them, what they do. Users answered even with the fake profile picture, a fact that makes us to realize how feasible it might be a Social Engineering attack.

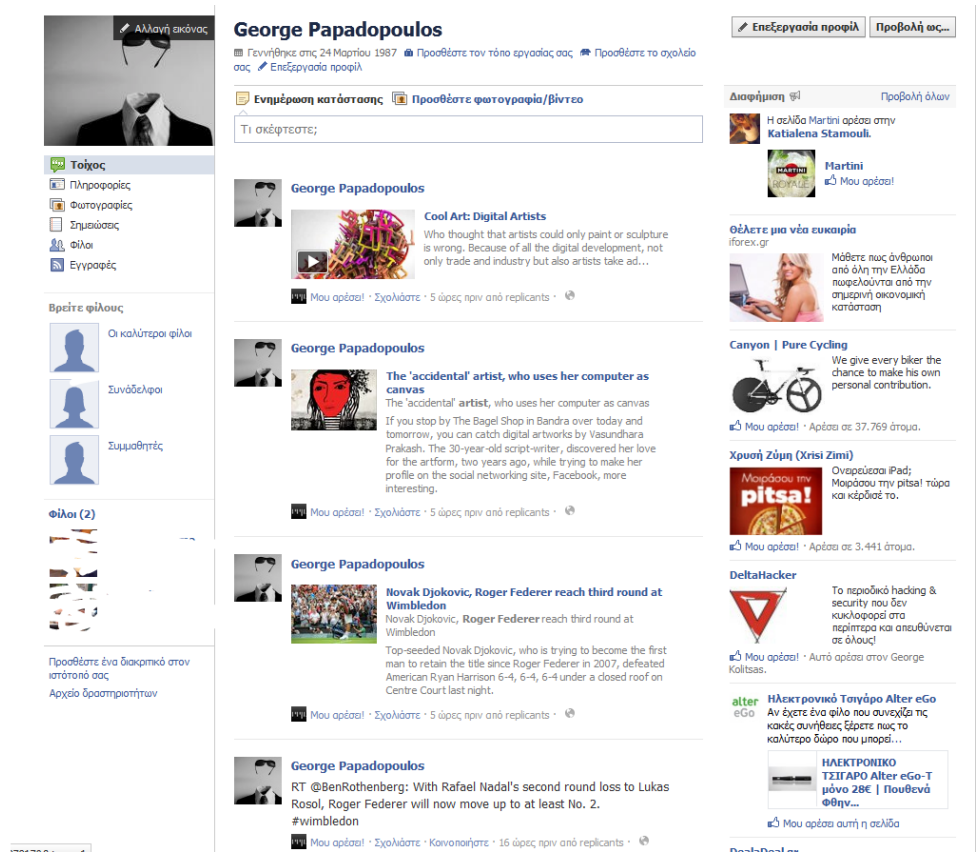


Figure 24.User's wall with the Replicants application

3.2 SOCIAL ENGINEERING

Social Engineering is the art of holding the weakest link in a security system that is the human factor. It refers to psychological manipulation of people in order to perform actions that do not really want. A social engineer tries to exploit his victims into revealing valuable information or tricks them so as to perform malicious acts on his behalf. This form of attacks makes the technical means that we use to protect ourselves, ineffective. Intruders are always on the lookout for ways to gain access to valuable resources such as computer systems, or corporate or personal information on them that can be used maliciously for the attackers' personal gain. Sometimes they get their chance when there are genuine gaps in the security that they can breach. Oftentimes, they get through because of human behaviors such as trust or ignorance. Attackers know how much easier it is to trick insiders instead of targeting the complex technological protections that we spend huge monetary sums on.

We can see two models of social engineering a trust model and an attack model.

The *Trust Model* describes how a social engineer establishes a trustworthy relationship with a person that has needed information for a social engineering attack. Initially, an attacker obtains background information about the target. A key early stage in the trust process is the receiver's judgment of the credibility of the information provided by the attacker.

There are three common areas to explain trust:

1. Trustor's propensity to trust.
2. Trustor's perception of the trustee's reputation, performance, and appearance.
3. The environmental circumstances.

Traits of the trustor will determine how easily that individual will trust another party. This is known as *propensity to trust*. The surrounding *environment* plays a vital role in convincing the trustor that the attacker is trustworthy. Environmental factors include the level of information being requested, the trustor's knowledge of its value, and the trustor's state of mind. *Trustworthiness* correlates with the motivation to lie. We recognize four factors that affect an attacker's perceived trustworthiness: benevolence, reputation, performance, and appearance.

The *Attack Model* illustrates how a single typical information-gathering attack is carried out to obtain a single item of information. Trust of a victim by an attacker is usually developed with the methods of the Trust Model as a precondition to most of the steps of the Attack Model. The model begins when the social engineer undertakes some research on the target individual or organization. The information gained, even if not helpful, may be used to obtain further information that might be helpful. Then the attacker uses one of a number of techniques to achieve their objective.

There are four main categories of attack techniques. They are deception, influence, persuasion and manipulation. The toolkit of a social engineering attack includes the tactics of friendliness, conformity, scarcity, sympathy, ignorance, and affiliation. Using some combination of these trust ploys to achieve one or more of these attack techniques, the social engineer tries to gain unauthorized access to systems or information. The intent is usually to commit a crime such as fraud, espionage, identity theft, or vandalism of a system or network. Depending on the size and other characteristics of the target information, the Attack Model can recurs until the goal is achieved.

3.3 GENERAL IMPLEMENTATION

As we mentioned in previous chapter, ChatBot is a program that accepts sentences as input in a natural language such as English and answers in the same language. The history goes back to 1951, where the British mathematician Alan Turing wondered whether machines can think. He proposed a test with the name "Turing Test", in which a computer and a person have a conversation with a third person and the last one had to distinguish the real one from his two interlocutors. Nowadays, this test was developed in a competition with the name "Loebner Prize" and it has a $ 100000 prize to those ChatBots that will fool a man for at least five minutes.

The "Turing Test" examined with great interest by Joseph Weizenbaum for the ELIZA program which was published in 1966 and it was seemed able to fool users into thinking that they are talking to a real person.

The key function of the program ELIZA, which was copied from the next year ChatBot creators, was that it was looking for words or sentences in the user's input and it was giving the output of ready programmed responses which could move the dialogue forward in a human manner. For instance, the user's input contains the word "Mother" will give the answer "Tell me more about your family". With all these we produce the illusion of understanding but essentially the piece of technical intelligence is superficial.

With the recent increase in the popularity of ChatBots there are many individuals that create their own ChatBots either for good purposes or for malicious ones. Creating our own ChatBot has many advantages and also disadvantages. There are pros and cons for stand-alone app and for a web-based ChatBot.

Some pros and cons for the stand-alone ChatBot applications:

1. They are simple to install and use them.
2. They have an attractive interface and a rich world to be explored.
3. Most of them have a "Text to speech" system which is very useful for our experience.

They have some cons, though:

1. These bots have limited degrees of configuration so they do not help you to personalize your bot.
2. Many times these applications are not free.
3. Many of them contain inappropriate content for children such as adult language or sexual situations.

Furthermore we can see some advantages and disadvantages concerned the web-based ChatBots:

1. Web-based ChatBots allow more control over behavior and personality.
2. We can choose if our bot can have inappropriate content, such as adult language or sexual situations, or not.

Unfortunately there are also some disadvantages:

1. It is more difficult to create a web-based ChatBot than a stand-alone one.
2. They require some programming experience such as to know HTML, CSS, JavaScript and AIML.

3.3.1 AIML

AIML (Artificial Intelligence Markup Language) is an XML language which is used to 'import' knowledge into ChatBots. It was developed by Dr. Richard Wallace (1995-2002) and was the basis for the development of a well known ChatBot named ALICE (Artificial Linguistic Internet Computer Entity). It was the evolution of ELIZA, a program which was created at MIT by Joseph Weizenbaum in 1964 and simulated a psychotherapist with whom everyone can chat, providing to the users a "real" human interaction. The free disposal of the ALICE code to the general public and also providing those with many free AIML Interpreters in different languages, such as Java or Python, had the effect of creating many ChatBot similar to Alicebot.

Figure 25.ELIZA ChatBot

(Source:http://www.planet-source-code.com/vb/scripts/ShowCode.asp?txtCodeId=5369&lngWId=3)

AIML is a very simple language to use. Describes a class of data objects in the name «AIML objects" and defines the behavior of the program used in their processing. The items are created by modules, which are called "categories". Each class consists of a question-input and a response-output. The question is defined as "pattern", while the answer as "template".

AIML also supports the use of various other tags, such as "system" or "JavaScript" and handles cases of synonymous words in questions, standard questions with few differences between them, recognizing spelling errors in questions and understand them.

"Categories" in AIML declare the fundamental units of knowledge. One category includes at least two more data, "pattern" and "template". A simple category is written as follows:

<aiml>

<category>

<pattern>WHAT IS YOUR NAME?</pattern>

<template>My name is <bot name="name"/>.</template>

</category>

</aiml>

When the above category runs, the AIML bot will respond in the input "What is your name" with the answer "My name is (the name of the bot)".

“Patterns” are a sequence of characters that are designed to fit one or more user’s input. The pattern "What is your name" will match only one entry ignoring if the characters are in uppercase or lowercase. The patterns can contain special characters such as: “What is your*” which will match an unlimited number of entries after the “What is your”.

“Templates” determine the answer to a matching pattern. Templates can be simple text or can contain variables such as: My name is <botname="name"/> which will put the bot's name in the sentence. Finally, they are able to switch to other patterns by using the item “srai”. This item is used when we have two different proposals with the same meaning and want to assign them in a template. For instance:

```
<category>

        <pattern>WHAT IS YOUR NAME</pattern>

        <template><![CDATA {My name is <bot name=”name”./>,]]></template>

</category>

<category>

        <pattern>WHAT ARE YOU CALLED</pattern>

        <template>

                <srai>what is your name</srai>

        </template>

</category>
```

The first category simply responds to input "what is your name" with the name of the bot. The second category tells us that the entrance of "what are you called" have to be redirected to the category "what is your name".

3.3.2 PYTHON

Now we have to see more specific the implementation of a ChatBot. The programming language that we will use for this purpose is Python. First it worth to be mentioned a few things about Python.

Python is a programming language and December 1989 Guido van Rossum started its implementation. Python 2.0 was released on 2000 and its 3.0 version on December 2008. Python is also free and open source software and fully supports object-oriented programming. A particular feature of the language is the use of whitespace for separating the syntax structure on the contrary to other languages which use special symbols such as brackets. This feature combined with the fact that it uses full English words in place of symbols, makes the Python code readable to those who have a basic knowledge in English. Moreover some of the statements that Python uses in its code are: if, for, while, try, import, yield, pass, assert, def, class and with. Last but not least it is worth to be mentioned that Python from 2008 is listed in the eight most popular programming languages.

Developing a ChatBot we will need first a Facebook account in order to use it for instant messaging. The ChatBot should be able to respond "intelligently" to inputs. This means great input parsing, understanding of context and large knowledge base.

So if we want to create our own ChatBot we need:

1. Language technology tools
2. Knowledge base
3. Context management
4. Experience & server

Another implementing tool that we will use is **PandoraBots**. The pandorabots.com is a free, open source community, which enables creating ChatBot on the Internet. The user has the ability to use ready code files and edit them as he desires or just to create from the begging his own. Afterward, user can train his bot through the provided graphical user interface where he asks questions and depending on the received answer, he accepts or rejects this response in order to train it as he wishes. Finally, he has the option to reveal the bot in order to use it for trial conversation with other users of the website.

3.4 INSTANT MESSAGING

Instant messaging (IM) is a type of online chat that offers to users a real time communication and a real time text transmission through the Internet. There is also the LAN messenger which operates in a similar way with the instant messaging, over a local area network. Instant messaging systems facilitate communications and connections between two or more users. Some of these systems allow users to send messages without being online, so they can send offline messages, which is the biggest difference between IM and Facebook chat. Users may send text messages to each other through these systems but also they can see and talk directly to each other via webcams and to send files and emoticons just like Facebook chat.

In 1990 instant messaging made its appearance on the Internet and it was a multi-user operating system such as the Compatible Time-Sharing System. During the years instant messaging systems developed in the form that we know today. It is worth to be mentioned that there is also the mobile instant messaging (MIM) which is a technology that is accessed to portable devices such as the smartphones which have operating systems like Android, iOS, Windows phone and so on.

Unfortunately, there are some security risks on using instant messaging which are similar with the risks when we use the social media. Hackers constantly use the instant messaging for malicious purposes. So attackers use the IM in order to deliver phising attempts. They have two methods to deliver malicious code or data through the IM which are:

1. The delivery of viruses and spyware.
2. The use of a web address which urges the user to click on this URL and when the user is connected with it, he downloads malicious code.

Moreover, the inappropriate use of IM in the workplace can cause serious problems to the employees. Companies now include the IM on their policies for the appropriate use of it, including the e-mail and other corporate issues.

The services are based on open protocol XMPP (eXtensible Messaging and Presence Protocol) of the IETF (Internet Engineering Task Force) and implemented through the server. The software that users have to install on their computer is, for instance a Jabber client, and most of them are freely available on the web.

3.4.1 The top 10 IM clients for Facebook chat

In this section we will get familiar and we will test these ten IM clients for Facebook chat which are:

1. Adium
2. AIM
3. Digsby
4. ICQ
5. Windows Live Messenger
6. Nimbuzz
7. Miranda IM
8. Pidgin
9. Trillian
10. Yahoo Messenger

These ten IM clients introduced a whole new way to chat without signing in with our web browser. Facebook chat is also an IM client but we cannot chat offsite. Now the evolution is that these IM clients support Facebook chat, so the users are no longer required to stay online on a social network so as to chat with their friends and their family.

Let's see in more details the top 10 IM clients.

- Adium

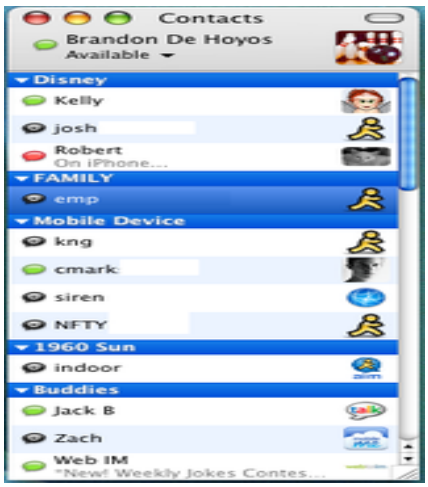


Figure 26.Adium IM

(Source:http://im.about.com/od/im-clients/a/facebook-chat-im-clients.htm)

Adium is one of the most popular IM clients that exist in the market. Its main disadvantage is that it is free and available only for Mac users and no for Windows users. Adium is a multi-protocol IM client which offers to its users the opportunity to include their Facebook chat users in only one single application.

By using Adium users can add multiple IM accounts, send and receive IMs, connect Facebook chat to Adium, share photos and files, chat with tabbed windows, share iTunes playlist in real time and receive Growl notifications.

If users want to add IM accounts to Adium they can do it upon installation of Adium. They can select the appropriate IM client from the services drop-down menu on their Adium Setup Assistant. Then they can fill out their corresponding screenname and password so as to continue. Once they do these steps, their IM contacts will appear to the Adium buddy list and the users will be ready to chat with any contact they want by simply clicking twice on it.

- AIM

Figure 27.AIM IM

(Source:http://im.about.com/od/im-clients/a/facebook-chat-im-clients.htm)

AIM is the most widely used IM program in America. It is estimated that is has over 53 million users. AIM one of the leaders in the IM market was the first program that allowed photo and file sending and also audio and webcam chat. AIM program is available for Mac users but also for Windows users (required to have Windows 2000 and higher) and for mobile phones.

Users of AIM program can send and receive IMs, save conversations with AIM files, share files and photos, sign-in to AIM with Facebook, upload photos for instant IM icons and connect Facebook chat to AIM 7.

If users want to start a conversation with another user, the only thing that they should do, is to select an IM contact and then to double-click on it. But if users want to start an AIM conversation with a user that do not exist on the buddy list, they should click on the "menu" and then to select "new IM". Continuing they will enter the buddy's screenname, then the text that they want to type and the conversation is ready to begin.

The most important part is to sign in to Facebook chat with AIM. Users can click on the Facebook icon on the bottom of their AIM buddy list. They should enter their Facebook information in order to login and then to click "allow" so as to give permission to access the AIM to your Facebook account. Finally, their Facebook contacts will appear on the AIM buddy list.

- Digsby

Figure 28.Digsby IM

(Source:http://im.about.com/od/im-clients/a/facebook-chat-im-clients.htm)

Digsby is one of the most simplest and easiest to use IM client. By using Digsby users can connect with MSN, Yahoo, Google Talk and Facebook chat accounts. With Digsby users can add IM contacts to Digsby IM, send and receive IMs, organize contacts in groups, manage multiple IM accounts, save Digsby IM chats, send files and access to social networking accounts.

Digsby users can also add their social networking accounts to the Digsby client by clicking "Add Social Network," and selecting the network of their choice. Next, Digsby users must fill their account information in the fields which is provided. If users want to add accounts to Digsby, they should click on “Digsby” on the menu and then to select “Add New Contact”. Next they can select their contacts from the drop-down menu in the field “Contact Type” and the connection is done.

- ICQ

Figure 29.ICQ IM

(Source:http://im.about.com/od/im-clients/a/facebook-chat-im-clients.htm)

ICQ was one of first IM clients and it still remains the most popular among the U.S. users. Nowadays, ICQ has over 42 million users. ICQ is available for Mac and Windows users and of course for mobile phones. With ICQ users can send and receive IMs, add contacts and groups to their ICQ buddy list, meet new friends in chat rooms, stay up to date on social network accounts, add buddy icons and create ICQ avatars.

Our main purpose is the connection of Facebook to our ICQ feed. The first step is to click the Feeds tab on our buddy list and then click the "Set Up Your Feeds" button to continue. Then we click on the button “Add” in order to add Facebook on ICQ and then the button “Connect”. Continuing we should log in to Facebook and click again “Connect”. Finally, we click on the "Allow Access" until we have completed the connection between Facebook and ICQ Feeds.

If users want to add contact on their buddy list, they should click on the option “Add contact” and then to enter the contact’s information which they want to connect with. Clicking on “Add” they have added the contacts they want.

- Windows Live Messenger

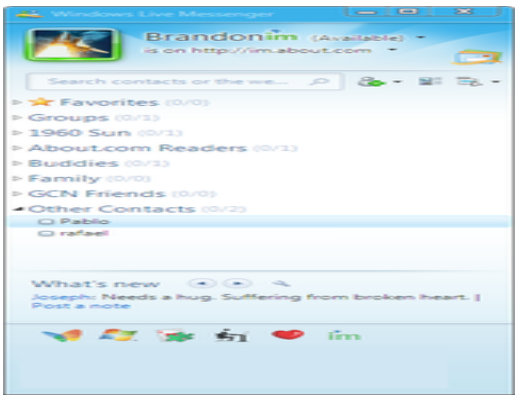


Figure 30.Windows Live Messenger

(Source:http://im.about.com/od/im-clients/a/facebook-chat-im-clients.htm)

Windows Live Messenger is second most popular IM client in America. It has more than 27 million users in all over the world. Calling it as Windows Live Messenger or as MSN is exactly the same thing. Windows Live Messenger is available for Windows users but Microsoft messenger for Mac is the same for Mac users. One import thing before begin Windows Live Messenger is that users should have Windows XP and higher.

Users who use Windows Live Messenger can sign up for a free Windows Live Messenger account, send and receive Windows Live Messenger IMs, add Windows Live Messenger contacts and create groups if they want, receive offline IMs, chat with Yahoo Messenger users, share files and photos and chat with gamers on the XBOX 360 system.

In addition, users can add new contacts on Windows Live Messenger. They will click on the icon "Find a contact…" and then they will add their friend's information. Before adding the new friend, users can choose in which group to place him in from their list. Once all the information has been placed, they will press "Add contact" and is done.

- Nimbuzz

Figure 31.Nimbuzz IM

(Source:http://im.about.com/od/im-clients/a/facebook-chat-im-clients.htm)

Nimbuzz made its appearance in May 2008. It is a very popular IM client as every three seconds a new member subscribed. Nimbuzz supports social networks such as Gtalk, Yahoo Messenger, Windows Live Messenger, MySpace, Skype, Facebook, Twitter and more. Users who use Nimbuzz can send IMs to their contacts, add new contacts to their Nimbuzz contacts list, connect Facebook Chat to Nimbuzz, call friends for free, share music, movies and photos and personalize IMs with IM icons.

Nimbuzz support IM clients on Windows, Mac, and mobile devices, including Symbian, iPhone, Windows Mobile, Android, and BlackBerry. It is also very simple to add Facebook chat to Nimbuzz. Users can select "Communities" and next click on the "Connect with Facebook". Next users should sign in to their Facebook chat from Nimbuzz. Then they will click "Allow" in order to allow Nimbuzz to access their Facebook chat account. Finally, they can start sending and receiving Nimbuzz IMs with their Facebook Chat friends without the need necessarily to sign in.

- Miranda IM

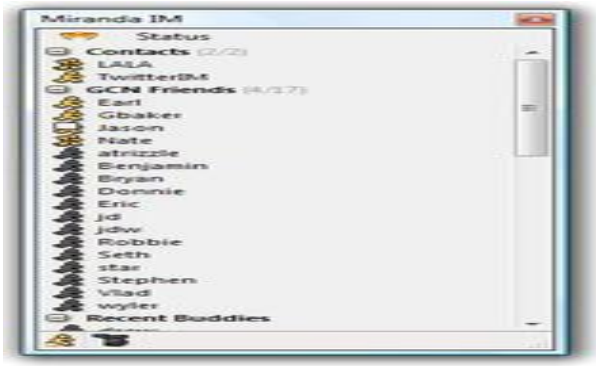


Figure 32.Miranda IM

(Source:http://im.about.com/od/im-clients/a/facebook-chat-im-clients.htm)

Miranda IM is a very easy and simple IM client to use. It offers multi-protocol support to IM clients including Yahoo Messenger, Windows Live Messenger and more. Miranda IM is available to Windows users but they should have Windows 95 and higher. Everyone who uses it can send and receive IMs, manage IM accounts, install support for emoticons and add over 350 Miranda IM plugins.

To begin setting up Miranda Messenger, right click to the Miranda Messenger icon, select "Main Menu," and then "Accounts." By doing this, users will be able to add IM accounts. Continuing users should select an IM protocol and finally the accounts have added to Miranda Messenger. One last step is to click to each individual IM client and enter their IM screenname and password.

- Pidgin

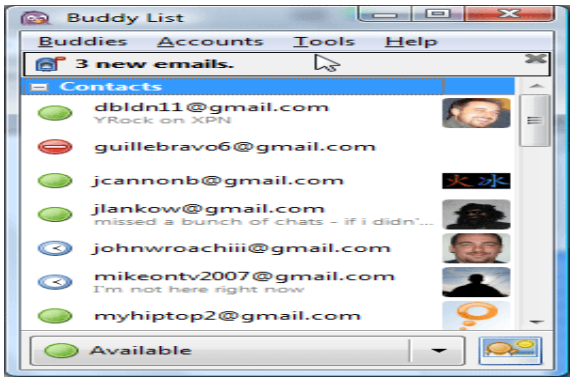


Figure 33.Pidgin IM

(Source:http://im.about.com/od/im-clients/a/facebook-chat-im-clients.htm)

Pidgin is an open-source platform that allows users to log into various services from one application. The number of the users of Pidgin was estimated in 3 million in 2007. Its formerly name was Gaim and it was released in 1998. Pidgin also supports many operating systems such as Windows, Linux, Mac OS and some more. Users that occupy with it can send and receive IMs, add IM contacts and organize them in groups, manage multiple IM accounts, save Pidgin IM chat logs, appear as invisible to IM contacts, transfer files and add Buddy Icons.

We can easily add Facebook chat to Pidgin. The first click is in the "Manage accounts" and then by clicking on "Add" we should select the XMPP protocol from the list. Next it will be asked to enter our username and our password. One of the most important steps are that we should click on the "Advanced tab" and uncheck the "Require SSL/TLS" box and also to make sure that the connect port will be 5222. Finally, by clicking "Add" our Facebook friends will show up directly in our buddy list.

- Trillian

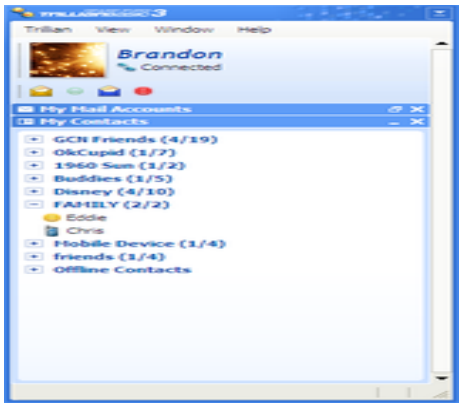


Figure 34.Trillian IM

(Source:http://im.about.com/od/im-clients/a/facebook-chat-im-clients.htm)

Trillian is the first multi-protocol IM clients and is known for its innovation as it offers one of the most popular IM clients in our days. Trillian users can have contact with users in Yahoo Messenger, Windows Live Messenger and AIM. With Trillian users can send and receive IMs, do voice chat, share photos and files, rename contacts for easier organization, host multiple-user chat rooms and utilize integrated web search.

Setting up Trillian is an easy procedure. After installing Trillian on our computers we should choose a nickname and an icon for our account. After choosing an identity we have the option to choose of accessing buddies form other IM clients. With the last step and by clicking "Ok" Trillian is ready to use.

- Yahoo Messenger

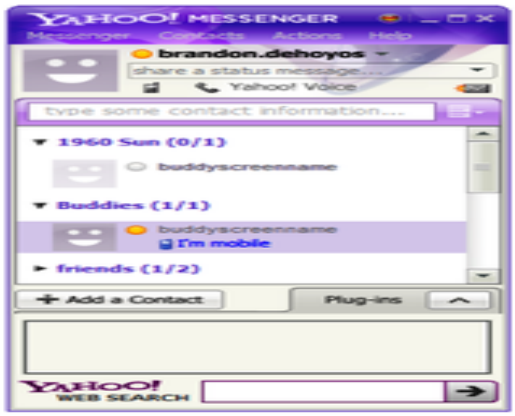


Figure 35.Yahoo Messenger

(Source:http://im.about.com/od/im-clients/a/facebook-chat-im-clients.htm)

Yahoo Messenger is the third largest IM client application in the world with 22 million users. Its initial release was in March 1998. Yahoo Messenger is available for Windows, Linux and Mac users. Users who use Yahoo Messenger can send and receive IMs, have communication through video and voice chat, share photos and videos, join lively discussions in Yahoo chat, make PC-to-phone calls for a low per-minute rate, accept messages offline and on mobile devices and personalize IM text/fonts and profiles.

Adding contacts on Yahoo Messenger is one of the most common functions. First users should click on "Contacts" on the toolbar and then select "Add a contact". Next users can enter their contact's Yahoo Messenger that they want to add. There is also the option to select a group they would like to add their contacts. Finally, a confirmation message will appear that will tell that the contacts have added successfully.

3.5 REQUIREMENTS ANALYISIS – SCENARIOS

The final aim of this thesis was the automated detection of Social Zombies. After thorough research we came to the idea of using a ChatBot and studying the communication through Facebook chat between a real user and the ChatBot. This was the initial scenario but having faced some technical difficulties during the implementation, we came up with a second scenario. The idea was the usage and the testing of the top 10 instant messaging applications. We connected them with Facebook chat in order to implement a conversation through these applications with another user who used Facebook chat. We tested if these applications were valuable when we were online and also offline of Facebook chat and moreover if all the facilities that they provide worked properly.

To implement the above scenarios were used the following requirements:

1. Use of a Facebook account.
2. Use of instant messaging applications (Adium, AIM, Digsby, ICQ, Windows Live Messenger, Nimbuzz, Miranda IM, Pidgin, Trillian, Yahoo Messenger).
3. Connection of IM applications with Facebook chat.
4. Use ChatBot for automated messaging.

The above requirements were covered by using the tools presented above. The exact description of how to use these will be followed by the analysis of the scenarios.

3.5.1 Scenario 1

For the scenario concerning the detection of Social Zombies by using a ChatBot and Facebook we followed the following steps:

1. We install the software of Python 2.7.3 in order to implement the appropriate changes to our ChatBot.
2. Then with the help of a Facebook chat we would had tried to implement our scenario.

Unfortunately, this venture did not end well and with the desired results. We faced difficulties with Python coding and the data that should had used on the code, so we did not get the appropriate results.

The code that was used for this scenario was:

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

import sleekxmpp
import logging
import cleverbot
#import dnspython

def session_start(event):
    chatbot.send_presence()
    print('Session started')
    chatbot.get_roster()

def message(msg):
    if msg['type'] in ('chat','normal'):
        #print "msg recieved"
        msg1 = msg['body']
        print(msg1)
        #print "from",msg['from']
        #msg.reply("Thanks").send()
        reply = cb.Ask(msg1)
        if not reply:
           reply = 'you said:'+msg1
        print('reply: ' + reply +'\n')
        msg.reply(reply).send()
        #msg.reply(reply).send()

jid = 'YOUR_FACEBOOK_LOGIN'
password = 'YOUR_FACEBOOK_PASSWORD'
addr = ('chat.facebook.com', 5222)
ipaddr = ('209.85.175.125',5222)

chatbot = sleekxmpp.ClientXMPP(jid,password)
chatbot.add_event_handler("session_start", session_start)
chatbot.add_event_handler("message", message)

chatbot.auto_reconnect = True
```

```
#logging.basicConfig(level=logging.DEBUG,
# format='%(levelname)-8s %(message)s')

cb = cleverbot.Session()

chatbot.connect(addr)
chatbot.process(threaded=False)
```

3.5.2 Scenario 2

Regarding the second scenario while chatting we implemented some controls and detections on these ten IM applications. We used two Facebook chats, one which was connected with the IM clients so as to chat through them and another one in order to be able to be implemented a conversation. The test was concerned:

1. Send/Receive IMs
2. Video calls
3. Voice calls
4. Share photos
5. Share files
6. Emoticons
7. Chat history
8. Social Networks

We had some observations before the final results of this test. First, the IM client "Adium" is only available for Mac users, so we did not manage to use it as we have Windows users. It also worth to be mentioned that "Windows Live Messenger" is now working through "Skype" application, so the connection with Facebook chat made through "Skype". Last but not least, there were some IM clients which did not provide quick login to Facebook chat. It was more complicated and time consuming than quick to login when we used "Miranda IM", "Pidgin" and "Nimbuzz" applications.

We implemented the testing on these ten IM clients and the results are shown in the table below:

	Send/ Receive IMs	Video calls	Voice calls	Share photos	Share files	Emoticons	Chat history	Social Networks
Adium	-	-	-	-	-	-	-	-
AIM	✓	x	x	x	x	✓	✓	✓
Digsby	✓	x	x	x	✓	✓	✓	✓
ICQ	✓	x	x	x	x	✓	✓	✓
Windows Live Messenger	✓	✓	✓	x	x	✓	✓	x
Nimbuzz	✓	x	x	✓	✓	✓	✓	✓

Miranda IM	✓	x	x	x	✓	✓	x	x
Pidgin	✓	x	x	✓	✓	✓	✓	✓
Trillian	✓	x	x	✓	✓	✓	✓	✓
Yahoo Messenger	✓	✓	x	✓	✓	✓	✓	✓

We can conclude by saying that we tested the compatibility between Facebook and the 10 IM applications and we found that most of them were quite useful and functional as Facebook chat, such as "Windows Live Messenger", "Pidgin" and "Trillian". Unfortunately, none of the ten IM applications completely supported the 8 features that we wanted to test. So, we summarize that the most appropriate application remains Facebook chat and there is no reason to be substituted by an application less effective.

CHAPTER 4: CONCLUSIONS

4.1 EVALUATION

We live in an era where the revolution of social media is a fact. The speed in which the changes in technological terms are staggering is high and our efforts to stop the development and the further expansion of social media is meaningless. As specifically Qualman (2009) said "is no longer our choice whether to use social media. The issue now is how well we will use them". Moving in this context and having accepted the benefits of social media, we can stand in front of the media seriously and responsibly. In an era dominated by information and audiovisual stimuli, it is necessary to cultivate critical thinking and demonstrate maturity against any malicious threat. The right training will lead us towards this direction via so-called "media literacy". With this way citizens will enable to become responsible users of the Internet, but also will have the ability to analyze, evaluate and create messages in a wide variety of media, online and offline. Then the active citizens of the Internet can perhaps be converted into participant citizens in an effective and active level for the protection of the rights and freedom of their expression.

After studying all those that are mentioned in the thesis and the survey that have conducted, we can conclude that social networking sites hide many risks for their users. It is certain that the operators of them are trying to ensure mainly their safety and then their privacy, and that the human factor plays the most important role on this. Nonetheless, it is proved that the road is still long and there is much work to be done, which increases as the number of users grows and the technology evolves. We should not forget the fact that social networking applications are also commonly used in Smartphone devices which is already a new target for many malicious Internet users. All the same, there are simple tools as we mentioned in our thesis which could create ways to detect and protect users.

4.2 PERSONAL REFLECTION

Since the beginning of the social media appearance, people became their major supporters. More and more people, regardless age, use the social networking applications. Facebook and Twitter are the most popular social media with the most subscribed users in world. This phenomenon is a little bit scary, as Internet users prefer to post personal data, personal opinions, photos of their everyday life and chat with people even if they are stranger. These users are characterized with the term "social zombies".

Unfortunately there are many Internet users who are willing to use all this information taken easily from the social media for malicious purposes. There are so many ways mentioned above that hackers can steal information from other users or perform an attack to users' computer when they are vulnerable, in order to cause technical damage. As we can see, social media which are not used properly and without security from their users, they can be transformed in nightmare.

Facebook and Facebook chat for instance which is the most overused social networking application, give so many functional opportunities to its users, such as to get in touch with people who already know, to make new friends and to get informed of whatever they want. I believe that except these opportunities, there are many malicious issues that dominate the good ones. First of all, Facebook faces lot of security problems and we had many incidents over the years. Moreover, even its operators allow its low security in order our personal data to be available to everyone, either they are commercial companies or other unknown users. For all these reasons, even it was for the dissertation purposes, I preferred not open a Facebook account and I used my sister's account.

Thus, we should consider the "game" which has been inverted between the social media and us as users, whereas we ended up to be more "clients" for the social media than we should be. To sum up, we should also think if the disadvantages of using the Social Media surpass the advantages and do something before it is too late.

4.3 FUTURE WORK

So far, we have studied how users interact on today's online social networks and observed how the trust and the interest of the Internet users can be used from hackers for malicious purposes. The explosion in popularity of social media underscores the continuing integration of computing in our daily lives, a trend that provides a number of interesting research challenges.

Users often share very personal information on social media, with little regard for who will be allowed to view the content. The underlying problem is, essentially, ensuring privacy for users while allowing them to share information and knowledge freely. This problem has aspects that extent to the areas of security. Thus, one challenge is to design mechanisms that enable the wide-spread sharing that user's desire while ensuring that users understand who else is able to access their content. One potential first step to solving this problem is to use security tools/applications as an idea for expressing privacy policies, allowing users to share content and chat carefree with more than just their friends but not necessarily with the entire world.

In this paper, we also tried to propose a method of automated detection of malicious user in the environment of Facebook by using ChatBot. This implementation can accept many extensions. For instance, using features of false accounts, we could use Semantics and Ontologies to evolve the bot in a Content-based detector via web-based application that checks users' profile. In case it located a combination of these features, it would alert the user. Finally, knowing that every social network has different infrastructure, it would be very useful to utilize also these applications to other networks beyond Facebook.

References

[1] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, Matei Ripeanu, The Socialbot Network: When Bots Socialize for Fame and Money, 2011

[2] Markus Huber, Stewart Kowalskiy, Marcus Nohlbergz, Simon Tjoa, Towards Automating Social Engineering Using Social Networking Sites, 2009

Bibliography

Websites:

1. http://blog.schipul.com/facebook-users-attacked-by-trojan-virus/
2. http://techchai.com/2011/04/05/how-to-identify-facebook-viruses-worms-and-fake-links/
3. http://news.bbc.co.uk/2/hi/7918839.stm
4. http://www.pcpowerguide.com/windows/is-your-computer-a-zombie/
5. http://news.cnet.com/8301-13739_3-9904331-46.html
6. http://www.slideshare.net/agent0x0/social-zombies-ii-your-friends-need-more-brains-3107346
7. http://www.slideshare.net/agent0x0/social-zombies-your-friends-want-to-eat-your-brains
8. http://www.sans.org/reading_room/whitepapers/email/spam-anti-spam_1776
9. http://www.sans.org/reading_room/whitepapers/email/is-affect-us-deal-spam_1111
10.
11. http://www.sysomos.com/insidetwitter/
12. http://www.guardian.co.uk/technology/blog/2009/aug/07/facebook-twitter
13. http://mashable.com/2009/08/06/twitter-bots/
14. http://techblog.gr/internet/koobface-worm-facebook-4291/
15. http://www.away.gr/2010/07/05/verisign-phising/
16. http://mattmckeon.com/facebook-privacy/
17. http://urbanlegends.about.com/b/2008/12/05/koobface-facebook-virus.htm

18. http://www.away.gr/2010/10/05/google-vs-facebook-infographic/
19. http://www.away.gr/2011/01/31/facebook-introduces-https-and-social-captcha/
20. http://www.away.gr/2011/02/09/tweets-can-be-reproduced-in-press-according-to-uk-court/
21. http://www.away.gr/2011/03/01/how-important-is-facebook-in-our-lives-infographic/
22. http://www.away.gr/2011/03/16/twitter-adds-more-security-with-default-https/
23. http://nakedsecurity.sophos.com/2011/01/09/facebook-photo-album-chat-messages-spreading-koobface-worm/
24. http://www.reuters.com/article/2010/03/18/us-facebook-virus-idUSTRE62G5A420100318
25. http://www.dailyfinance.com/2009/06/10/dont-let-this-facebook-virus-happen-to-you/
26. http://allfacebook.com/new-facebook-image-virus_b9338
27. http://www.hercampus.com/life/facebook-viruses-how-get-rid-them
28. http://www.moneymagpie.com/article/311/financial-fraud/
29. http://www.slideshare.net/agent0x0/social-zombies-ii-your-friends-need-more-brains-3107346
30. http://www.slideshare.net/agent0x0/social-zombies-gone-wild-totally-exposed-and-uncensored-7664492
31. http://www.slideshare.net/clauwa/socialbots-www2012

32. http://www.newscientist.com/article/mg20928045.100-fake-tweets-by-socialbot-fool-hundreds-of-followers.html
33. http://blog.zeltser.com/post/2822651353/bots-chatting-on-social-networks
34. http://blog.zeltser.com/post/2810171253/bots-control-social-networking-content
35. http://blog.zeltser.com/post/7010401548/bots-command-and-control-via-social-media
36. http://www.ethnos.gr/article.asp?catid=22768&subid=2&pubid=63655882
37. http://psychografimata.com/11498/apoplanisi-meso-diadiktiou-grooming/
38. http://www.tovima.gr/society/article/?aid=442413
39. http://internet-safety.sch.gr/index.php/ekp/162-repeu
40. http://ariadni.med.uoa.gr/
41. http://im.about.com/od/im-clients/a/facebook-chat-im-clients.htm