Salesian Journal on Information Systems
n. 16 (2015) pp. 71-81

SISTEMAS DE INFORMAÇÃO
http://www.fsma.edu.br/si/sistemas.html

TRILHA PRINCIPAL

Qualitative Characterization of the Facebook Information Security Strategies

Silmara Ferreira Lopes[1], Glívia Angélica Rodrigues Barbosa[2], Marcelo Werneck Barbosa[1]
[1]Computer Science and Exact Sciences Institute – PUC Minas
[2]Computer Science Department – CEFET Minas
silmara.lopes@sga.pucminas.br, gliviabarbosa@decom.cefetmg.br, mwerneck@pucminas.br

***Abstract*—Hyperconnectivity due to online social networks exposed security issues on data stored in these systems. This article presents an analysis on how online social networks designers have been communicating information security aspects through these systems' interfaces. This analysis was made using the Semiotic Inspection Method on Facebook since it is largely used in Brazil and all over the world. Results showed that there is major concern with security information properties. Nevertheless it was possible to identify interface problems that could compromise use and understanding of such security properties.**

***Index terms* - Semiotic Inspection Method. Social networks. Information Security**

I. Introduction

According to the Communications and Information Technologies Study Center [6], given the large advances in technology, we have instantaneous access to information. Coupled to this easiness, come several threats, attacks and crimes, which may cause huge moral, financial and even physical damage to organizations and people. These studies also point out to a continuous growth along the last years of the number of information security incidents.

Albesher e Alhussain [1] present studies that show that research performed in the Field of Information Security is more focused on technological and mathematical aspects and little has been written on the social aspects of Information Security. Organizations have technology towards this goal and create policies, norms and procedures that are technically correct but are essentially incomplete, given that they do not deal correctly with the human relations involved, allowing for attacks such as Social Engineering.

Social networks are a social structure made of persons or organizations, connected by one or several types of relationships that share values and common goals [10]. An online social network, on the other hand, is a platform that offers a communication and digital interaction space to a set of persons with similar needs and interests [11].

Online social networks are web based applications that people use to connect to other people with whom they share common interests, both personal and professional. Users publish contents in the application in order to update connections and share personal news, interests and other contents. These can be done in the form of simple texts, photos or videos.

People use social networks to find jobs, new customers or get in touch with distant friends or family. Examples of online social networks include LinkedIn, Facebook, Twitter and YouTube. Online social networks usually offer additional applications that extend their functionality, such as games or quizzes, which are usually developed by partners and can potentially incur in security risks [17], when they, for instance, ask for information from your account in order to provide the functionality. Situations like this can cause a profile invasion of information leaks. Given the growth of online social networks, the problem due to the vulnerability on security and information privacy issues becomes stronger. Personal information exposition is still potentially huge.

Cases such as the Playstation network penetration in 2011 allow us to assume that any online application that stores information online can become a target of attacks. In this paper we will focus only on online social networks, but this does not mean that the concepts presented here are not extensible to other network types.

Social media companies such as Facebook, Google and Twitter usually have their own privacy policies that rule the usage of client data and the conduct of third parties in their networks when dealing with personal data [4]. Nevertheless, the social networks themselves do not make it clear what their privacy policies are, putting the user in risk, as pointed out by a study made by the Brazilian Institute for Consumer Protection [14]. In an analysis made on the most popular social networks in Brazil, including Facebook [7], the study showed that even though the network does not charge for its services, users are compelled to input their personal information without being aware of what will be done with it and tend to accept use conditions.

In a certain way, this is similar to what a physical store does, which allows us to say that both situations are risky. Nevertheless, in the case of social networks the reach of the exposure is potentially bigger, given that the information is shared in a faster and more agile way. Besides, in a social network it may be difficult to pinpoint the origin of an information leak, among other problems inherent to its architecture and conception.

Security and privacy when dealing with social network sites are fundamentally behavioral and not technological issues. The more information a person posts, the more information is available for undue use or for malicious purposes. Publishing photos, videos or audio files can take to the loss of individual privacy [17].

The main responsible for privacy and security is the user himself. Information posted may propagate and something that could be a joke among friends can be accessed by other persons and used against the user now or in the future [18]. Nevertheless, even though this is mainly the user's responsibility , the technological solution must offer mechanisms for the user himself to protect the security of his own information [36][37].

In the last years, the popularity of social networks has grown immensely [9], [15]. Nevertheless, social networks do not attract users of good faith, but also those of bad intentions [15]. Hence, protecting privacy, sharing information and application in online social networks or in the Internet are very important problems [33].

This is such an important need that recently Facebook has announced new privacy configurations. In spite of these great advances, researchers and specialists continue to criticize those configurations, for they need to be improved and simplified [33].

On the other hand the topic of information security in online social networks has not received the due attention in academic research, as shown by Albuquerque and Santos [2], who performed an analysis of the Brazilian publications on information security in scientific journals from 2004 up to 2013. The research showed that few of the analyzed journals published papers on information security in the last 10 years and that those papers usually focus on the importance of norms and standards for information security

Given this context, there are doubts about how the data provided by the users will be manipulated. This paper is based on the premise that those doubts may be related to interface problems, given that the interface and interaction designer might not be able to correctly communicate his intentions to the users. Hence, persons that use the Facebook need some previous knowledge and some type of experience with software and web systems interfaces in order to correctly use the software.

Hence, this work consists in analyzing how the designer communicates through the system interface the information security properties inside the Facebook social network. In order to achieve this, we used the Qualitative Semiotic Inspection Method [22], and based on the results found, we presented the way the properties communication is made to the user, as well as the strategies adopted by the designer and the potential security problems that could afflict the users during their interaction with the system.

The results of this analysis and characterization can guide the improvement and/or the development of solutions that improve information security in social networks, given that they identify the strategies used by Facebook and identify the interface problems related to the presentation of security issues.

The remainder of this work is organized as follows. Section 2 presents the related works. Section 3 describes the methodological procedures adopted, as well as the theoretical framework. Section 4 presents the appreciation of the Facebook information security proposal, as well as the security breaches identified in this paper, and Section 5 describes conclusions and future works.

II. Related Works

There are ways to protect the privacy, control security, relationships status and other information and categorize lists of friends in order to limit undue access. The study performed by Yuksel, Yuksel and Zaim [33] provides an implementation of a web solution to protect information privacy. This solution helps users to automatically categorize a great number of friends into classification lists. The main premise in this paper is that users tend to present the same information to all their friends in a social group and hence, social circles provide a way to categorize friends and establish security and privacy policies. The approach is based on the construction of a visual graph of social groups and in the establishment of policies to protect personal information. This approach suggests the set of lists of friends that should be created and how the current friends should be divided into those lists.

The work by Ngeno et al. [19] replicated a small scale research that focused in users with a high degree of knowledge and interest in IT and in the expression of their needs and requirements. Using a series of interviews, some users were invited to report their experiences with social network sites. Based on the answers given, it could be seen that the interviewees wish for more transparency, trust and privacy within Facebook. The authors of this research came to the conclusion that the interviewees are conscious of the problems and in a certain way accept Facebook security problems.

The work in [38] analyzed how pharmacy students performed their privacy configuration before and after being aware of Facebook security policies. The work showed that after knowing the policy, the students opted for safer configurations and that publicizing the policy had a positive impact on these students' behavior.

The research performed by Dhami et al. [9] intended to understand the impact of safety, trust and privacy concerns when sharing information on social network sites. Using online forms, empirical data was collected from 250 users in Facebook from different age groups during a 4 month period. The findings from this research suggest that a factor that affected trust in Facebook was the safety characteristics it provided and an individual belief that accessing the Facebook through the Internet is safe. It was also realized that there is a strong correlation between the users' perceived privacy and their perceived trust.

The work by Albesher and Alhussain [1] intended to improve the protection of users' personal sensitive information at social network sites. The work discussed in particular privacy configuration issues, security issues and third party application within Facebook. The results of the paper highlight the need for regular reviews of the privacy configurations.

The work by Binden et al. [4] highlights the importance of configuring in an appropriate way the privacy configurations. Since more and more users are paying less attention to the privacy configurations, it is recommended to change the standard configurations in social networks to the safest possible in order to avoid leaking personal information.

There are also some papers that discuss attacks in social networks such as those by Hasib [13], Malagi, Angadi and Gull [17] or even by Zilpelwar, Bedi and Wadhai [34]. Most papers in this area present attacks to online social networks and show that privacy of user information is a big concern in those networks, even if, in general, these papers do not present useful solutions to protect information privacy [33]. Besides, none of them tried to evaluate how the network designer communicates the security related information to its users.

III. Methodology and Theoretical Framework

Considering our goal, we looked to investigate the following research question: *"How does the designer communicate through the system interface the information security properties in Facebook social network?"*.

The methodology used to answer this question consisted in a qualitative approach, divided into two steps. The first one looked to investigate which the security options communicated in the Facebook interface are. The second step looked to investigate which the relationship between the possibilities offered by the designer of this social network and the information security pillars is (described in Section IIIB). In order to perform the above mentioned analysis, we used the Semiotic Inspection Method (SIM) [22], which will be described in the next section.

A. Semiotic Inspection Method

The Semiotic Inspection Method (SIM) is based on the Theory of Semiotic Engineering (SemEng) [31] and is a theory that explains the Human Computer Interaction (HCI). It allows us to understand the phenomena involved in the design, usage and evaluation of an interactive system [22]. SemEng offers explanations for the phenomena that occur in the design, usage and evaluation of an interactive system and focuses on the communication process between the designer and the user through the system interface.

In SemEng, the system interface is seen as an instance of metacommunication (that is, the communication between the designer and the user), where it is communicated to the user through this interface the designer view on who is the target of this interface and which problems he can solve by interacting with it. The message that the designer transmits to the user is known as the metamessage and is understood by the user as he interacts with the interface. According to Souza [31], the interface of a system is a message from the designer to the user, whose content is:

"This is my interpretation on Who you are and I understood about what you want or need to do, which ways do you prefer to do it and why. Here, therefore, is the system that as a consequence I develop to you, which you can or should user this way, in order to perform a series of goals associated with this vision (of mine)".

The metamessage the designer sends to the user is made by signs. A sign is everything that means something to someone [21]. SemEng identifies three types of signs: metalinguistic, static and dynamic. Metalinguistic signs are those that refer to other interface signs and are used by the designers to communicate to users the meanings coded in the system and how to use them (for instance, documentation and help system). Static signs are those that express the state of the system. They can be interpreted just by looking at the interface (for instance, buttons that allow closing or minimizing a window, icon of a folder in the workspace or a magnifying glass drawing in the research field at a browser). The dynamic signs, from their part, express the behavior of the system and can only be perceived as the user interacts with it (for instance, an exclusion button becomes enabled when we select an e-mail in Outlook).

SIM is a method based in SemEng [31] for the evaluation of interactive systems. SIM analyzes the interface from the point of view of the designer metacommunication message emission. The goal of SIM is to identify if there are communication breaches (that is, problems) and to allow the evaluators to rebuild the designer metamessage, which is composed by signs that are the interface elements.

In order to evaluate an interface, SIM proposes 5 steps that must be followed by the evaluator: (1) inspection of the metalinguistic signs; (2) inspection of the static signs; (3) inspection of the dynamic signs; (4) contrast and compare between the messages identified in each of the inspections and (5) appreciate the quality of the metacommunication.

The inspection of the metalinguistic sign consists of a step defined in the SIM that is used in our methodology. The inspection is performed by experts in order to verify the actual explicit information on the system, which are not restricted to the help system, are clear and sufficient for the user to understand the system. According to the proponents of this method, this phase is extremely important because even though users do not usually use these instructions at first, they might be useful when questions arise during the interaction between users and system.

In the three initial steps, the evaluator must reconstruct the metamessage from the designer. The use of the periphrasis mentioned in the beginning of this topic is suggested as a template. At the fourth step, an analysis of the metacommunication messages generated in the previous step is made. Finally, at the last step we perform an evaluation of the communicability of the inspected system.

SIM was adopted for the evaluation proposed here because even though the method was originally proposed to evaluate the communicability of systems, a literature review performed by Reis and Prates [25] showed that this method also allows the identification of design strategies communicated in a system interface whose goal is to increase the potential specific usage qualities and/or properties (like sociability or privacy) [24][3].

In this sense, the work performed by Coutinho, Prates and Chaimowicz [8], identifies sound strategies for game orientation through the use of SIM. On the other hand, the work performed by Barbosa, Santos and Pereira [3] used SIM to identify sociability strategies in social networks. The authors Silva and Oliveira [30] used SIM to identify marketing strategies in hotel sites and, finally, the work performed by Silva and Barbosa [29] adopts this method to characterize gamification strategies in education mobile applications.

These works justify using SIM because they show the application of this method in similar contexts, allowing for the extrapolation for the case under study.

All these evidences justify using SIM in the identification of security strategies communicated at the Facebook interface. Based on this analysis, the decisions from this social network designers were compared with security strategies available in the literature in order to verify if Facebook contemplates the minimum security requirements. In order to better understand strategies, the next section describes concepts related to information security, as well as properties that are necessary for it.

B. *Information Security and Security Strategies*

Information security can be understood as a set of practices and measures, all intended to duly protect information and data, having as a common goal the preservation of its integrity, confidentiality and availability [16]. Information security can be defined as a knowledge area dedicated to protect information assets against unauthorized access, undue changes or information unavailability. The set of these three problems forms what we are calling security and will be analyzed using the SIM method.

We can also define security as a practice adopted to make an environment safe (activity, action or principles preservation), of multidisciplinary character, made of a set of methodologies and applications that intend to establish security control (for instance, authentication, authorization and auditing) of the elements that make up a communication network and/or manipulate information [28].

Every piece of information is an asset and each asset has a unique value to the organization and/or individual and hence, must be duly protected against several types of threats to keep its integrity, availability, confidentiality, authenticity and legality, those being the information properties [28].

In this context of protection and preservation of information, it is necessary to understand the meaning of a security system and which pillars and principles guide its implementation. According to Sêmola [28], information security can be implemented by a set of five properties, as follows:

- Integrity, which is related to how we protect information against undue, change, either accidental or in purpose;
- Availability corresponds to the fact that the information is accessible at the moment an individual or organization needs it;
- Confidentiality is related to the degree of information protection according to the degree of secrecy associated with its content;
- Authenticity may be related to an identification process, a way to guarantee that the involved parts are exactly who they claim to be;
- Finally, legality is associated to the respect of legal aspects, such as laws, norms and policies.

Notice that these aspects were analyzed based on what was communicated in the interface. We did not start specifically from them, but analyzed the interface in order to verify whether or not they were present at the social network.

Among the aspects observed by Information Security is the privacy of user data, which some authors, such as Sêmola [28], see as part of confidentiality. Privacy can be understood as the information set about the individual which he may decide to keep under his control or communicate, deciding who will be the recipient, when, where and under which conditions he will communicate, without being legally obliged to do so [5].

These concepts take on specific nuances in online social networks. Concerning integrity, most social networks allow only the account owner used to authenticate into the system may alter or delete data. These permissions cannot be passed on to other network users, making it difficult for a non authorized change of data to happen. This way, on the concept of integrity, there is not a large concern from most mechanisms of access control in social networks about the modification or exclusion of data from a user made by an unauthorized users, because to do so it would be necessary to know the login and the password of the user account, in order to authenticate into the system and make the unauthorized changes [27]. These problems may be extrapolated to any access to data within computer systems, but the focus of this work relies solely on social networks.

On the issue of confidentiality of the personal information stored in the users' profiles, most networks use a mechanism based on the relationship level between the user and the person who wants to access the data. In some networks, such as Facebook, the relationship level is divided in, for instance, All, Friends of Friends, Friends or personalized list. The data can also be marked as private, being accessible only to the account owner. This mechanism is very popular, because it provides a good balance between flexibility and ease of use and can capture a certain level of trust that a user has with those that belong to his network [27].

Sharing great amounts of information (including text, photos and any other type of content) brings security and privacy problems for social network users [33]. The information privacy issue has received growing attention. Close to 25% of the Americans consider themselves victims because the privacy of their information has been violated [9].

A valid discussion is whether people who share such a large amount of information really have an expectation of privacy. It must be understood that the goal of this work is to evaluate what the tool offers in terms of protection and security of the data so that the user can easily decide which level of protection he wants for his information. We agree that there is a human component in the issue, but this does not preclude the technology to play its part in helping the user. This concept can be seen explicitly in [38], where students in a Pharmacy college began to use better the security configurations after they got to know the corresponding policies.

Many persons beyond your friends and colleagues are interested in information that you post in social networks. Identity thieves, information thieves, stalkers and corporations are seeking a competitive advantage using social networks to gather information on the consumers. In this scenario, we have the violation of property authenticity, that is, the emitter of the information is not who he claims to be. In the same scenario, we can also have violations of other properties, such as legality, because information usage should be according to the applicable laws, regulations, licenses and contract. We can even have a violation of the availability, because information may not always be available to use when the authorized users need it [28].

Organizations that operate on social networks are gathering a multitude of data on their users, both to personalize their services and to sell it to advertisers, as announces in the Facebook own data policy [12]. The concern about information leak and security and privacy breaches has grown in the social networks environment [15].

Some people could argue that nobody reads the license agreement and that this would give rights to Facebook, in what amounts to a tacit authorization. This is an interesting point and the discussion here is whether this is explicit and clear in the user interface. We understand that there is a difference in not doing because of ignorance and not doing while being aware of the configurations, but opting not to use them. This works focuses only in the first case.

In the next section we present the main results of our investigation.

IV. Analysis and Discussion of the Facebook Security Proposal

In this section we will present an analysis of the Facebook Interface performed using SIM, indicating the designer proposal for information security in this social network, as well as the strategies he adopted.

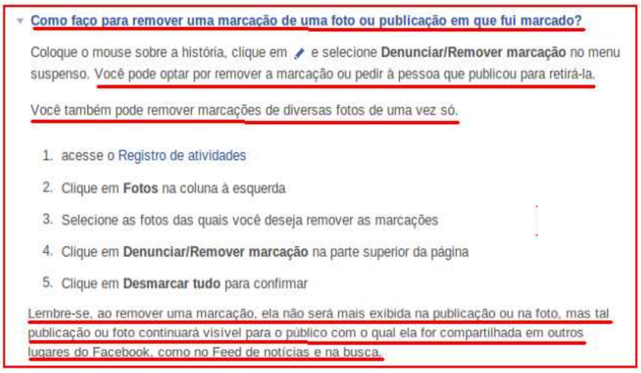
The evaluation was performed in a period of nine days (from September 6th, 2014 to September 15th, 2014) and conducted by the two authors of this paper. One of them had already performed other interface evaluations of social software using the method here proposed [3].

The scope was limited to the Brazilian version in Portuguese and the following tasks: (1) perform login using password; (2) visualize a content in the time line; (3) visualize a picture; (4) comment on the content of a *post*; (5) publishing a post in the time line; (6) configure account privacy; (7) configure account security and (8) talk using the chat.

The choice of scenarios was made because these are directly related to the information security properties in Facebook. Figures 1, 2 and 3 presented ahead show examples of the inspected signs. It is important to point out that we highlighted in each figure the interface aspects that make it evident what will be presented as the designer security proposal.

In order to appreciate the metalinguistic signs, we analyzed the system help, sub-topics login, password, privacy and personal data. Figure 1 shows an example of the metalinguisting sign inspected in the Facebook which contains instructions to the user on how to remove a marking in a picture or publication in which he was marked.

The static signs were analyzed based on the elements that make the timeline, the newsfeed, the photo album, the privacy configuration and the exchange on instant messages between users (chat). Figure 2 shows an example of an inspected static sign that contains interface elements that indicate the possibility of publishing a comment, picture of marking a user in a specific place.



Como faço para remover uma marcação de uma foto ou publicação em que fui marcado?

Coloque o mouse sobre a história, clique em ✎ e selecione **Denunciar/Remover marcação** no menu suspenso. Você pode optar por remover a marcação ou pedir à pessoa que publicou para retirá-la.

Você também pode remover marcações de diversas fotos de uma vez só.

1. acesse o Registro de atividades
2. Clique em **Fotos** na coluna à esquerda
3. Selecione as fotos das quais você deseja remover as marcações
4. Clique em **Denunciar/Remover marcação** na parte superior da página
5. Clique em **Desmarcar tudo** para confirmar

Lembre-se, ao remover uma marcação, ela não será mais exibida na publicação ou na foto, mas tal publicação ou foto continuará visível para o público com o qual ela for compartilhada em outros lugares do Facebook, como no Feed de notícias e na busca.

Fig. 1. Evidence of the evaluation of a metalinguistic sign.

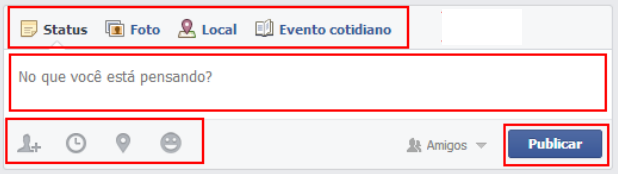
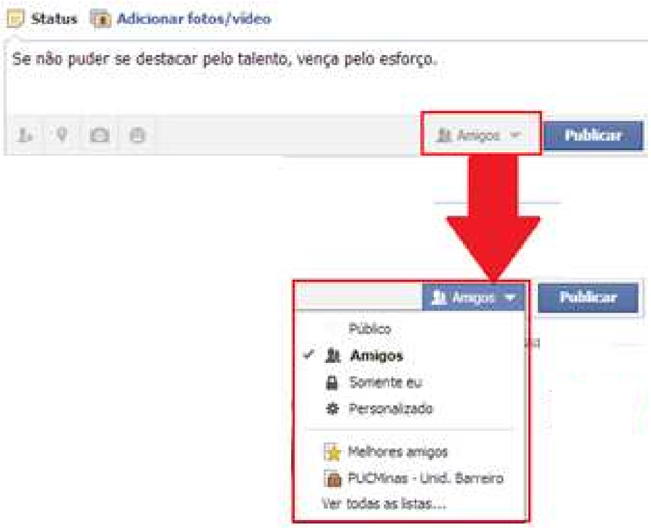


Fig. 2. Evidence of the evaluation of a static sign.

Finally, the dynamic signs were appreciated through the interaction with the resources proposed for content sharing, user communication and privacy configuration. Figure 3 shows an example of a dynamic sign inspected in Facebook that allows the user to change the visibility of a published content.



Se não puder se destacar pelo talento, vença pelo esforço.

Fig. 3. Evidence of evaluation of a dynamic sign.

The results found with the application of SIM and the juxtaposition of the three metamessages corresponding to the evaluation of dynamic, static and metalinguistic symbols in a final message will be presented in the next section.

A. Facebook Information Security Proposal

Based on the inspection to identify the system metamessage, we verified that the purpose of Facebook designer is to offer to its users a space where it is possible to share contents (such as texts, videos, messages and images) and interact with other people.

The system has policies and use terms that, as reported by the designer himself in a metamessage, should be follow because: "*given that Facebook offers people around the world the power to publish their own stories, see the world through the eyes of many others and connect and share wherever they are. The conversation that occurs inside Facebook – and the opinions expressed here – reflects the diversity of people that use it. In order to balance the needs and the interests of a global population, Facebook protects the expression that adheres to the community standards described in this page*".

Any person who has an e-mail and accepts the terms and policies is allowed to create an account in Facebook and start to use its services. By creating a profile, the user can make available information on: (1) Work and education; (2) Residence; (3) Relationship (that is, if you are single, have a boyfriend/girlfriend, is engaged, married or separated); (4) Family (that is, which of your family members are in Facebook and which is your degree of relationship with them); (5) Contacts (that is, e-mail and telephone numbers); among other information, such as favorite TV shows, songs, movies and books. Besides, it is possible to publish an image whose goal is to visually identify the profile owner.

Out of these pieces of information, the designer demands only that the user provides an unique identifying name to represent him.

For the interaction among members to happen, the Facebook designer offers a tool to search and locate persons and another to recommend friends. In order to begin a friendship with another member, the owner of the profile has two options: (1) send a friendship request to someone who may or may not accept it; (2) accept the friendship request from another member. In order to organize the friends the user has in its profile, the designer offers the possibility to group them into lists or even to specify some possible degree of kinship.

The main resources offered for interaction and content sharing between the owner of the profile and his friends are the newsfeed (or mural), instant messages (or chat), events and groups. The user can publish content both in his newsfeed and/or in his friend's newsfeed, as long as he got the permission to do so. Sharing can be done through text, image and/or video. Besides, it is possible to include information such as data, location or even to mark friends.

Once we identified the metamessage from Facebook to its users, and considering the information security properties, it was possible to verify that the designer addresses security aspects in its interface, with the goal to support a safe social interaction among its members.

Among the designer decisions connected with security, we can highlight the control over the shared content exhibition in the user profile. The visibility of the newsfeed publications, as well as that of the personal information, is under control of the profile owner. He must decide whether this content is public, restricted to friends, private (visible only to himself) or personalized. This way, if the published content is not private, his friends can like, comment or even share it with other persons. It is important to point out that the user can control only what is visible through his profile, and not is visible through his friends' profiles.

Another relevant decision on security is the possibility to accept or refuse friendship requests, which allows the user to control who has access to his profile. This does not happen in other networks, such as Google+ and Twitter. Facebook also allows the user to configure permissions over markings and publications made by third parties in a profile. In this case, before the publication is shown in the newsfeed, the profile owner decides whether or not the content should be visible. Nevertheless, even if the user does not authorize the exhibition, the content can be seen in the profile of the person who created it.

It should also be noticed that Facebook also allows denouncing content so that it becomes excluded forever. Nevertheless, given the need for human analysis, the time between the publication and the solution of the denunciation is enough for the information to propagate online.

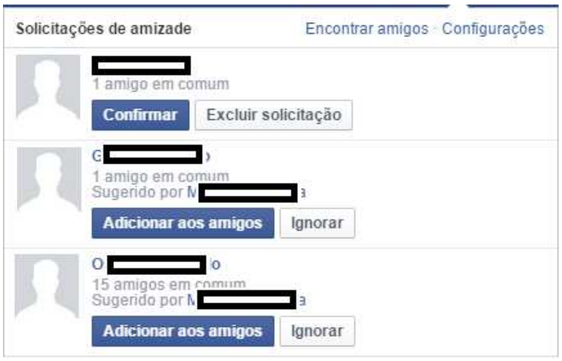
Finally, in terms of availability and with the goal of insuring a good relationship between users who keep in touch through Facebook, the designer notifies each member about updates that happen in his problem. For instance, when a friendship request or a message is sent to the member, or even, when someone shares, comments or likes his newsfeed, the user receives a notification in real time so that he has the opportunity to offer a feedback to the person or group that interacted with him (for instance, answer a message, like a content or accept a friendship request).

Once we identified the Facebook designer proposal in terms of security, in the next section we present the strategies adopted to promote this property in the system.

B. *Identified Information Security Strategies*

Based on the Facebook security proposal identified with SIM, it was possible to realize that the designer uses strategies that consider the information security pillars presented in Section IIIB. Table 1 presents the identified strategies that are aligned with the security properties presented above, as well as the designer decisions (point out by SIM), which make clear those decisions in Facebook. We should point out that in some cases the same strategy reflects different designer decisions. Next, we will present some examples of how those strategies were implemented in Facebook.

Figure 4 shows an example of strategy implementation identified as D2 in Table 1, which is related to the Authenticity property of information security. This designer decision is related to the authenticity property because the user can verify and identify who is sending the friendship requests.



Solicitações de amizade
Encontrar amigos · Configurações

[redacted]
1 amigo em comum
Confirmar
Excluir solicitação

[redacted]
1 amigo em comum
Sugerido por [redacted]
Adicionar aos amigos
Ignorar

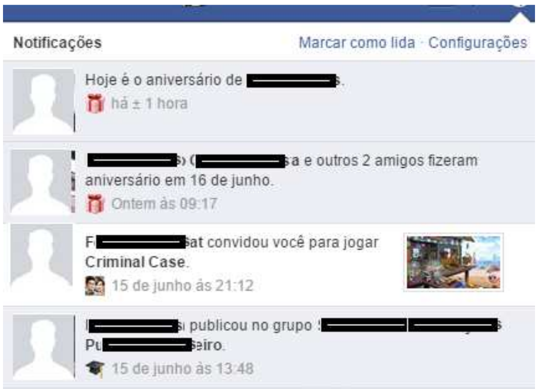
[redacted]
15 amigos em comum
Sugerido por [redacted]
Adicionar aos amigos
Ignorar

Fig. 4. Evidence of the D2 designer decision.

TABLE 1
INFORMATION SECURITY STRATEGIES IN FACEBOOK

Information Security Strategy/Property	Designer Decision	Justification in the context of information security
E1 – Autenticity	D1 – *Login* and password to access Facebook	Identifies the user who is using Facebook. Guarantees that the user is really who he claims to be. For instance, that the user is the one who created the account and has access authorization (but not necessarily who he claims to be in his profile).
	D2 – Approve friendship request.	Guarantees to the user the possibility of choosing with whom He wishes to have a relationship (that is, communicate/exchange information) in the social network. This way, the user can verify the source and the recipient of the contents that will be shared/visualized at his profile.
E2 – Confidenciality	D3 – Definition of content visibility/privacy in the profile.	Guarantees to the user control on who has access to his personal information and to his shared contents. In other words, the user defines the degree of secrecy of each information
E3 – Availability	D4 – Notification of profile updates in real time.	Makes available in real time notifications about updates that happened in the user profile (for instance, friendship requests, mural publications). This decision allows the user to provide a feedback to the person or group that interacted with him.
E4 – Integrity	D5 – Analyze third party markings before exhibiting them in the user profile.	Guarantees to the user the possibility of deciding if it is convenient or not to publish contents in his profile that were not originally submitted by him (for instance, shared by a friend) and verifying before publication if the content is intact (for instance, if it was not altered or manipulated unduly).
E5 – Legality	D6 – Denounce non proper content.	Allows the user to denounce contents that do not follow the Facebook usage, security or privacy policies. This way, it is sought to guarantee that the content and behavior inside the social network follow the norms and laws.

Figure 5 shows an example of the implementation of the strategy identified as D4 in Table 1, which is related to the Availability property of information security. This figure shows how a user can visualize in real time notifications about updates that happened in his profile. This way, the user can provide feedback to the person or group that interacted with him.



Notificações Marcar como lida · Configurações

Hoje é o aniversário de [redacted].
há ± 1 hora

[redacted] ([redacted]a e outros 2 amigos fizeram aniversário em 16 de junho.
Ontem às 09:17

F[redacted]at convidou você para jogar Criminal Case.
15 de junho às 21:12

[redacted] publicou no grupo [redacted] Pu[redacted]eiro.
15 de junho às 13:48

Fig. 5. Evidence of the D4 designer decision.

Figure 6 shows an example of the implementation of the strategy identified as D6 in Table 1, which is related to the Legality property of information security. Figure 6 shows how the user can denounce contents that do not follow the usage, security and/or privacy Facebook policies. This way, it is sought to guarantee that the content and behavior inside the social network is guided by norms and laws. Figure 6 also makes it evident that there is the possibility of deciding, either by direct request or recommendation, if the user wishes to keep the contact in his network or not.

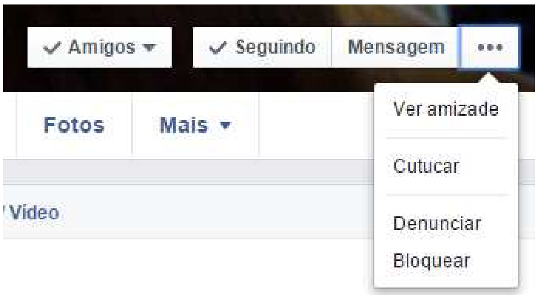


Fig. 6. Evidence of the D6 designer decision.

Once we finished this step of strategy identification, it was possible to verify that the designer offers resources that foster and make it possible to establish information security between Facebook members and that for this goal he adopts some security strategies (for instance, properties) considered as relevant in the context of interface project for systems who intend to foster a computer mediated social interaction in a secure way.

As we previously pointed out, the main goal of this work is to characterize the security strategies communicated in the Facebook interface. Nevertheless, in a complementary work, we sought to identify the potential problems (ruptures) that could be experienced by the users concerning security. In the next section these results are summarized and discussed.

C. Ruptures Found

In this section we will describe the main ruptures (RP) found by SIM and discuss the potential impact each one of them may have in the security of the user in Facebook. It is important to point out that the arguments used to explain the possible problems were based in [26], which discusses the impact of online systems security breaches.

RP1. Lack of clarity for access to security configurations. There is a section in Facebook called “How to connect” which has a set of questions directly connected to security and privacy configurations. Hence, the current section name is not consistent with the questions content, given that it does not suggest that in this space it is possible to find information concerning safety configurations. This rupture can cause an impact on the users’ security because by not realizing that the network offers resources that help in these configurations, the user may not perform a configuration or solve a doubt related to the security in Facebook and hence become vulnerable in this social network, which could possible cause a confidentiality or even integrity breach.

RP2. Using ambiguous terms. The designer uses ambiguous terms to express the same concepts in the Portuguese version of the system. One example of this ambiguity is the use of “Privacy Policy” to access security configurations, which can be considered a broader term than the one used. These ambiguities may hinder or even make impossible to identify and use the resources available in Facebook to configure security aspects of the network, maybe causing confidentiality breaches.

RP3. Excessive number of steps to access help on security configurations. In case the user has doubts and needs to access the Facebook help to get information on network security, he faces an excessive number of steps to get to the desired information (at least 7 clicks). This is a problem because it violates a basic principle of interface usability, the recognition instead of memorization [20][23]. In this case the user needs to memorize the path to access information and because it is so long, it may render the search non viable, compromising the correct use of configurations, in the case the doubts remain.

RP4. Limitation of the content visibility options. Even though Facebook offers a mechanism for the user to configure the visibility of the content show in his profile (for instance, text, photos and vídeos published in his newsfeed), there is no explicit way to control the content exhibited in a friend's newsfeed, in the case this content mentions another user. This decision causes an impact on security, given that a person can be exposed by another, even if not intentionally, causing a breach of confidentiality of his personal information.

RP5. Restriction of denunciation only to users who have a Facebook account. Facebook offers the possibility of denouncing profiles that do not respect its usage rules (for instance, fake profiles). Nevertheless, in the case of a fake profile, this denunciation is restricted to users who have a Facebook account. This happens because even though Facebook makes available instructions to denounce a fake account through the help page "Como faço para denunciar uma conta falsa?" (https://www.facebook.com/help/167722253287296), the options listed are visible only to users logged (that is, those who have an account) into Facebook. In other words, if the user who had his profile falsified accesses the above mentioned page from this false page, even though he can see the page, the denunciation option is not available. In this case, there can be the undue use of name and data from a person who has its name used to create a false account and does not have an account in Facebook.

V. Final Conclusions and Future Works

In this paper, the research question consisted in analyzing how the designer communicates the information security properties inside the context of a social network.

In this context, it was possible to come to the conclusion that, according to the final metamessage, the Facebook designer sought to improve information security in this system, incorporating in its interface in complementary way, the properties considered as the "security pillars". Nevertheless, some properties were made more evident (for instance, confidentiality) than others. For instance, it is not possible to identify information that allows the user to find easily the Facebook usage terms, and hence the Legality property is little, if ever, explored.

Hence, we can see that in a social network, for instance, for the designer it would be more important to keep the confidentiality than the availability, but this does not indicate that he does not addresses it, but yet that it does not devotes more resources to make it evident.

In terms of contribution, in spite of presenting a case study within Facebook, the appreciation performed is relevant both in practical terms as well in scientific/methodological terms for the areas of Human Computer Interaction (HCI) and Information Security.

In practical terms, the results contribute to the improvement and/or development of solutions that improve the information security in social networks. That is a consequence of the fact that this paper offers a perspective on information security strategies communicated in the Facebook interface which can also be adopted in other networks.

In scientific/methodological terms, the results from SIM reinforce the method applicability, because of its theoretical foundations, to identify design strategies communicated in the interface who intend to improve certain usage qualities (in this case, information security).

It should be noted at this moment that it impossible to come to the conclusion whether Facebook is good or not in relation to its criteria. The scope of this work focused in presenting what exists in term of resources and problems from the point of view of an expert in interaction. Even though this analysis is important and necessary, it allows us to identify evidence that must be confirmed through a triangulation made with studies with users. Hence, we understand that the conclusion should be made only after this study, as predicted to be included in the future studies.

As a proposal to future works, we pretend to evaluate under the user point of view, through the Communicability Evaluation Method (CEM), which is the perception about the information security properties and whether Facebook strategies support the users in this aspect.

Besides, another point to investigate is the possibility to identify interface signs that allow us to classify the information security possibilities offered by the online social networks. This would help in the project and the evaluation of other networks, such as Instagram. Hence, we will be able to demonstrate that our approach is applicable to several social networks, and not just a peculiarity of Facebook.

References

[1] A. Albesher and T.Alhussain. "Privacy and security issues in social networks: an evaluation of Facebook". *Proceedings of the 2013 International Conference on Information Systems and Design of Communication (ISDOC),* pp. 7-10, 2013.

[2] A. E. Albuquerque Júnior and E. M dos Santos. "Análise das Publicações Brasileiras sobre Segurança da Informação sob a Ótica Social em Periódicos Científicos entre 2004 e 2013". In: *XXXVIII Encontro da ANPAD, ENANPAD*, 2014, Rio de Janeiro.

[3] G. A. R . Barbosa, G. E. Santos and V. M. Pereira. "Caracterização Qualitativa da Sociabilidade no Facebook". In *Proceedings of XII Simpósio de Fatores Humanos em Sistemas Computacionais - IHC* 2013, Manaus, AM. .

[4] W. Binden, M. Jormae, Z. Zain and J. Ibrahim. "Employing Information Security Awareness to Minimize Over-Exposure of Average Internet User on Social Networks". *International Journal of Scientific and Research Publications*, Volume 4, Issue 1, Janeiro de 2014.

[5] C. E. B. A. Bragança, E. M. Luciano, M. G. Testa. "Segurança da Informação e privacidade de informações de pacientes de instituições de saúde: uma análise exploratória da priacidade percebida pelos profissionais". *XXXIV Encontro da ANPAD (ENANPAD),* 2010.

[6] CERT.BR. "Estatísticas dos Incidentes Reportados ao CERT.br. 1999 a junho de 2013". Disponível em: http://www.cert.br/stats/incidentes. Acesso em 02/06/2015.

[7] COMSCORE. "Facebook Blasts into Top Position in Brazilian Social Networking Market Following Year of Tremendous Growth". 2012. Disponível em <http://goo.gl/TcXcM>. Acesso em 02/06/2015.

[8] F. Coutinho, R. O. Prates, L. Chaimowicz. "An analysis of information conveyed through audio in an fps game and its impact on deaf players experience". In: *IEEE. Games and Digital Entertainment (SBGAMES),* 2011.

[9] A. Dhami, N. Agarwal, T. K. Chakraborty, B. P. Singh, J. Minj. "Impact of trust, security and privacy concerns in social networking:

An exploratory study to understand the pattern of information revelation in Facebook". In *3rd IEEE International Advance Computing Conference (IACC).* 2013.

[10] F. Duarte, C. Quandt. "O tempo das redes in redes urbanas". São Paulo, Brasil: Editora Perspectiva, 2008.

[11] N. B. Ellison, C. Steinfield and C. Lampe. "The benefits of Facebook "friends:" Social capital and college students' use of online social network sites". *Journal of Computer Mediated Communication*, 12(4), 1143-1168, 2007.

[12] Facebook. Política de Dados. Disponível em https://www.facebook.com/about/privacy/. Acesso em 19/10/2015.

[13] A. A. Hasib. "Threats of online social networks". Helsinki , Finland : Helsinki University of Technology. 2008.

[14] IDEC - Instituto Brasileiro de Defesa do Consumidor . 2012. "Pesquisa Quem vê seu perfil?" Disponível em http://www.idec.org.br/uploads/revistas_materias/pdfs/172-pesquisa-redes-sociais1.pdf. Acesso em 02/06/2015.

[15] M. R. Khayyambashi and F. S. Rizi. "An approach for detecting profile cloning in online social networks". In *7th International Conference on e-commerce on developing countries with focus on e-security*. 2013.

[16] ITSMF. "Fundamentos do Gerenciamento de Serviços em TI baseados no ITIL". Holanda: Van Haren Publishing, 2006.

[17] K. Malagi, A. Angadi and K. Gull. "A Survey on Security Issues and Concerns to Social Networks". I*nternational Journal of Science and Research (IJSR)*, India Online ISSN: 2319-7064 Volume 2 Issue 5, Maio 2013.

[18] E. S. Martins, F. J. V. Lucas and R. C. S. Vasconcelos. "Segurança da informação nas redes sociais". *Revista Sinergia,* São Paulo, v. 15, n. 4, p. 272-278, out./dez. 2014.

[19] C. Ngeno, P. Zavarsky, D. Lindskog and R. Ruhl. "User's Perspective: Privacy and Security of Information on Social Networks". In *IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust*. 2010.

[20] J. Nielsen. "Heuristic evaluation". In: J. Nielsen e R. L. Mack (Eds.) *Usability inspection methods*. New York: John Wiley & Sons, 1994. p. 25–62.

[21] C. S. Peirce. "The Essential Peirce". Indiana University Press, Bloomington, 1992.

[22] R. O. Prates, S. D. J. Barbosa. "Introdução à Teoria e Prática da Interação Humano Computador fundamentada na Engenharia Semiótica". *Jornada de Atualização em Informática (JAI),* Congresso da SBC, 2007.

[23] R. O. Prates e S. Barbosa. Avaliação de Interfaces de Usuário–Conceitos e Métodos. In:*Anais do XXIII Congresso Nacional da Sociedade Brasileira de Computação. XXII Jornadas de Atualização em Informática (JAI).* SBC 2003.

[24] J. Preece. "Online communities: Usability, Sociability, Theory and Methods". In R. Earnshaw, R. Guedj, A. van Dam and T. Vince (Eds) *Frontiers of Human-Centred Computing, Online Communities and Virtual Environmen*ts. 2001

[25] S. D. S. Reis and R. O. Prates. "Applicability of the semiotic inspection method: a systematic literature review". In Proce*edings of the X Symposium on Human Factors in Computing Systems and V Latin American Conference on Human Computer Interaction, IHC & CLIHC,* 2011.

[26] A. Santos and A. Andrade. "Portais de bibliotecas sistemas de avaliação de qualidade dos serviços". *Información, cultura y sociedad*, no 22, 2010.

[27] V. S. Santos, E. Porto and B. "Alturas. Análise de mecanismos de controle de acesso nas redes". *Revista Portuguesa e Brasileira de Gestão*, Vol. 9, No. 3, pp.50-60, ISSN: 1645-4464, 2010.

[28] M. Sêmola. "Gestão da Segurança da Informação: Uma visão executiva". 5. ed. Rio de Janeiro: Campus-Elsevier, 2003.

[29] J. C. R. da Silva; G. A. R. Barbosa. "Estratégias de gamificação como fator motivacional para o uso de aplicativos móveis educacionais:Um estudo de caso do aplicativo duolingo". *Simpósio Mineiro de Engenharia de Software (SMES)*. Belo Horizonte, Minas Gerais, 2014.

[30] M. C. F. Silva and A. Oliveira. "Marketing communication strategies for the corporate website of promenade champagnat: Using MIS at tourism". *Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais,* 2014.

[31] C. S. de Souza. "The semiotic engineering of human-computer interaction". MIT Press, 2005.

[32] C. S. de Souza, C. S. Leitão, R. O. Prates and E. J. da Silva. "The semiotic inspection method". In *Proceedings of VII Brazilian symposium on Human factors in computing systems (IHC '06)*. ACM, New York, NY, USA, 148-157, 2006.

[33] A. S. Yuksel, M. E. Yuksel and A. H. Zaim. "An Approach for Protecting Privacy on Social Networks". *Fifth International Conference on Systems and Networks Communications.* 2010.

[34] R. A.Zilpelwar, R. K. Bedi, and V. M. Wadhai. An Overview of Privacy and Security in SNS. International Journal of P2P Network Trends and Technology- Volume2 Issue1- 2012.

[35] N. B. X. Silva.; W. J. de Araújo and P. M. de Azevedo. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. Revista Ibero-americana de Ciência da Informação, v. 6, n. 2, p. 37-55, ago./dez. 2013

[36] J. Preece. Sociability and usability in online communities: Determining and measuring success. Behaviour & Information Technology. Behaviour & Information Technology 20, 5, (2001), 347–356.

[37] R. Pereira; M. C. C. Baranauskas and S. R. P. da Silva. Softwares sociais: uma visão orientada a valores. In Proc. of the IX Symposium on Human Factors in Computing Systems, IHC '10, (2010), 149-158.

[38] J. Williams; C. Feild and K. James. The Effects of a Social Media Policy on Pharmacy Students' Facebook Security Settings. American Journal of Pharmaceutical Education, v. 75, n.9, 2011.