Security Metrics In Social Networking Applications

Ulaa Alhaddad, Dr. Wajdi Al jedaibi

Abstract: Participation in social networking sites has dramatically increased in recent years. Social networking sites like Facebook1 or MySpace allow users to keep in touch with their friends, communicate and share content, ideas, activities, recommendations, with them, as well as engage in other multiuser applications. Services allow millions of individuals to create online profile and share personal information with vast networks of friends and often, unknown numbers of strangers. There are potential attacks on various aspects of user privacy. It is not well understood how privacy concern and trust influence social interactions within social networking sites. The continuous number of high-profile Internet security breaches reported in the mass media shows that despite an emphasis on security processes that there is still a gap between theory and practice. I intend in this research paper to propose a new model base on suggested model on social networking analysis and suggest a new security metrics to improve security and reduce the risks associated with users.

Keyword: Social network sites SNS, Design Patterns, Security Social network, multilevel model, friend of friend (FOF), Malicious, defense measures and security model.

1. Introduction

The phenomenon of social networking sites (SNS) introduced to the public about five to six years ago have changed the way people communicate with each other on the Internet. Some social networking sites like Facebook attracted millions of users in the first years of their operation and their operators claim to have hundreds of millions of users worldwide. The main benefit of the majority of social networks is to facilitate new friendships, online interaction and communication for which the user profile is the crucial component for establishing connections. In the profile a user can share information such as his name, photos, address, interests, political views, etc. Several studies showed that the members of social networks not only disclose true information about themselves, but provide even more information than they would do in real life [1, 2]. With the development of information retrieval and search engine techniques, it becomes very convenient to extract users' personal information that is readily available in various social networks. Malicious or curious users take advantage of these techniques to collect others' private information. Therefore, it is critical to enable users to control their information disclosure and effectively maintain security over online social networks. So, privacy, and other ethical and statutory obligations, generally imposes collections of system goals, each of which is managed in its own right. For example, a business goal of 'comply with data protection and human rights legislation' is interpreted as a list of security goals that are contained within statutes and related documentation (advice, orders), or established as best practice.

- *Ulaa Alhaddad, 1103803, Ulaa.alhaddad@gmail.com*
- *Supervisor: Dr. Wajdi Al jedaibi, Faculty of Computing & Information Technology King Abdul Aziz University, Jeddah*

These include protection goals (e.g.confidentiality and integrity of personal data) as well as functional requirements (e.g. users must be able to access and correct records held about themselves, data must be deleted after use).As a consequence there is no distinctive goal of 'privacy' that requires special treatment; each of these obligations are treated as a separate system goals. Security is difficult to measure because so many security attributes are not mutually commensurable. Perhaps for this reason, network security is often measured in terms of Information Assurance (IA). There are further complications we need to keep in mind, however, in this search for meaningful metrics. Therefore, I first review social network methodology, then in the second section I refer to comparison of two security patterns and I introduced common attacks in these networks. At last, I propose a security evaluation model for social networks systems. Finally, in the last section I concluded with conclusion and future work.

2. Literature review

Mark Zuckerberg launched Facebook, currently the most popular social networking site worldwide, only in February 2004. In January 2010, Mark Zuckerberg, the CEO of Facebook, stated at a technology conference that privacy is no longer a "social norm," as users have adapted to sharing information online over blogs and other social media and, in turn, the company has structured its privacy settings accordingly.2 Trust is defined in (Mayer, Davis, and Schoorman, 1995) as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trust or irrespective of the ability to monitor or control that other party". For face to face, trust is a critical determinant of sharing information and developing new relationships (Fukuyama,1995, Lewis and Weigert, 1985). Trust is also important for successful online interactions (Coppola, Hiltz, and Rotter, 2004, Jarvenpaa and Leidner, 1998, Meyerson 1996 Piccoli and Ives, 2003). Privacy within social networking sites is often not expected or is undefined (Dwyer, 2007). Social networking sites record all interactions, and retain them for potential use in social data mining. Offline, most social transactions leave behind no trace. This lack of a record is a passive enabler of social privacy (Lessig, 1998). Therefore these sites need explicit policies and data protection mechanisms in order to deliver the same level of social privacy found offline. Since online

social privacy is harder to warranty, does a higher level of concern for internet privacy affect the use of social networking sites? Levitt and Cheung [3] presented the common techniques used in faulttolerance and security. They provided security counterparts to the most common fault-tolerance terms. Meadows [4] presented an outline of a fault model for security and showed how it could be applied to both fault tolerance and fault forecasting in computer security. Jonsson [5][6] proposed an integrated framework for security and dependability from the viewpoint of behavioral and preventive terms. Meadows and Mclean [7] surveyed each part of the taxonomy for fault tolerance and described the research and practices in security that corresponded to it. Avizienis et al. [8] refined the concept of dependability and security by emphasizing on security. In the other hand we should consider Social network analysis [SNA] is the mapping and measuring of relationships and flows between people, groups, organizations, computers, URLs, and other connected information/knowledge entities. The nodes in the network are the people and groups while the links show relationships or flows between the nodes (Fig.1). Social network analysis (related to network theory) has emerged as a key technique in modern sociology. It has also gained a significant following in anthropology, biology, communication studies, economics, geography, information science, organizational studies, social psychology, and sociolinguistics, and has become a popular topic of speculation and study .Also Several analytic tendencies distinguish social network analysis. There is no assumption that groups are the building blocks of society, the approach is open to studying less bounded social systems, from nonlocal communities to links among websites.

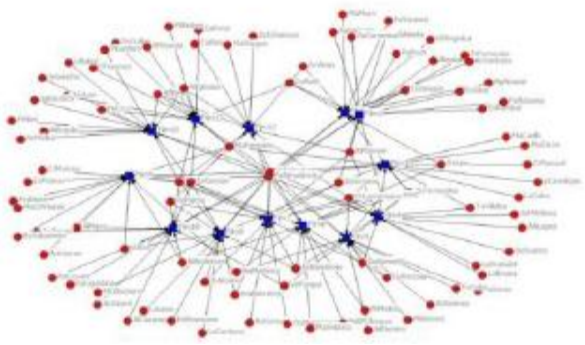

Figure 1: social network structure

Rather than treating individuals (persons, organizations, states) as discrete units of analysis, it focuses on how the structure of ties affects individuals and their relationships. In contrast to analyses that assume that socialization into norms determines behavior, network analysis looks to see the extent to which the structure and composition of ties affect norms. AS mentioned there are Metrics (Measures) in social network analyses. This are listed below:

Betweenness:
The extent to which a node lies between other nodes in the network. This measure takes into account the connectivity of the node's neighbors, giving a higher value for nodes which bridge clusters. The measure reflects the number of people who a person is connecting indirectly through their direct links.

Bridge:
An edge is said to be a bridge if deleting it would cause its endpoints to lie in different components of a graph.

Centrality:
This measure gives a rough indication of the social power of a node based on how well they "connect" the network. "Betweenness", "Closeness" and "Degree" are all measures of centrality.

Centralization:
The difference between the numbers of links for each node divided by maximum possible sum of differences. A centralized network will have many of its links dispersed around one or a few nodes, while a decentralized network is one in which there is little variation between the numbers of links each node possesses.

Closeness:
The degree an individual is near all other individuals in a network (directly or indirectly). It reflects the ability to access information through the "grapevine" of network members. Thus, closeness is the inverse of the sum of the shortest distances between each individual and every other person in the network.

Clustering coefficient:
A measure of the likelihood that two associates of a node are associates them. A higher clustering coefficient indicates a greater 'cliquishness'.

Cohesion:
The degree to which actors are connected directly to each other by cohesive bonds. Groups are identified as ‘cliques’ if every individual is directly tied to every other individual, ‘social circles’ if there is less stringency of direct contact, which is imprecise, or as structurally cohesive blocks if precision is wanted.

Degree:
The count of the number of ties to other actors in the network. This may also be known as the "geodesic distance". See also degree (graph theory).

(Individual-level) Density:
The degree a respondent's ties know one another/ proportion of ties among an individual's nominees. Network or global level density is the proportion of ties in a network relative to the total number possible (sparse versus dense networks).

Flow betweenness centrality:
The degree that a node contributes to sum of maximum flow between all pairs of nodes (not that node).

Eigenvector centrality:
A measure of the importance of a node in a network. It assigns relative scores to all nodes in the network based on the principle that connections to nodes having a high score contribute more to the score of the node in question.

Local Bridge:
An edge is a local bridge if its endpoints share no common neighbors. Unlike a bridge, a local bridge is contained in a cycle.

Path Length:
The distances between pairs of nodes in the network. Average path-length is the average of these distances between all pairs of nodes.

Prestige:
In a directed graph prestige is the term used to describe a node's centrality. "Degree Prestige", "Proximity Prestige", and "Status Prestige" are all measures of Prestige. See also degree (graph theory).

Radiality:
Degree an individual's network reaches out into the network and provides novel information and influence.

Reach:
The degree any member of a network can reach other members of the network. Structural cohesion: The minimum number of members who, if removed from a group, would disconnect the group.

Structural equivalence:
Refers to the extent to which nodes have a common set of linkages to other nodes in the system. The nodes don't need to have any ties to each other to be structurally equivalent.

Structural hole:
Static holes that can be strategically filled by connecting one or more link to link together other points. Linked to ideas of social capital: if you link to two people who are not linked you can control their communication. We inspire from Multilevel Security pattern as ancestor pattern to categories group of friend.

3. Security Metrics

Since security systems are of a different nature than other systems such functional or (AI) system, there is a need for developing security measure that addresses the specific character of such features. I shall adopt the following definition of Security Metrics "At a high-level, metrics are quantifiable measurements of some aspect of a system or enterprise. For an entity (system, product, or other) for which security is a meaningful concept, there are some identifiable attributes that collectively characterize the security of that entity. Further, a security metric (or combination of security metrics) is a quantitative measure of how much of that attribute the entity possesses. A security metric can be built from lower-level physical measures [9]. One of the most important aspects of any security architecture model is the ability to manage/maintain an accurate and consistent level of security controls. An integrated risk management program is critical in securing business objectives requiring the enforcement of confidentiality, integrity, availability, and accountability.

Confidentiality
Confidentiality ensures the protection of data from unauthorized access to a personal's information, which extends to all data directly associated with the architecture's applications, data stores, communication links and/or processes.

Integrity
Integrity ensures that data, services, and other controlled resources are not altered and/or destroyed in an unauthorized manner. Integrity based controls provide safeguards against accidental, unauthorized, or malicious actions that could result in the alteration of security protection mechanisms, security classification levels, addressing or routing information, and/or audit information.

Availability
Availability ensures the reliable and correct operation of information and system resources for which the loss of information and/or resource access would cause adverse results. Availability based security requirements include controls to prevent, detect, and/or monitor accidental, unauthorized, and/or malicious activities that could negatively impact the availability of critical information. Availability = the probability of a service request gets fulfilled

Accountability
Accountability requirements ensure that events can be associated to specific users and/or processes responsible for those actions. The overall goal is to be able to verify, with 100% certainty, that a particular electronic message can be associated with a particular individual, just as a handwritten signature on a bank check is tied back to the account owner. Accountability based controls include identification and authentication mechanisms, and access control. Most of the security attributes such as confidentiality and integrity are terms of qualities. In measuring such quality terms, an inherent difficulty is that there might be many different interpretations of what they really mean. Therefore, we must clearly articulate how these quality terms are to be defined. One way to do this is to define a model associated with the attribute to be measured. For example, confidentiality of information has always played a central role in networks security. Unauthorized disclosure of information, if not prevented, may cause catastrophic results. In general, good cryptography combined with physical security is often considered to be our best answer to the problem. We use a factor-criteria model to describe confidentiality. Figure 2 depicts such a model. It divides confidentiality into three main factors: cryptographic protection, physical security and software access control. These factors are then further broken into a set of lower level criteria.

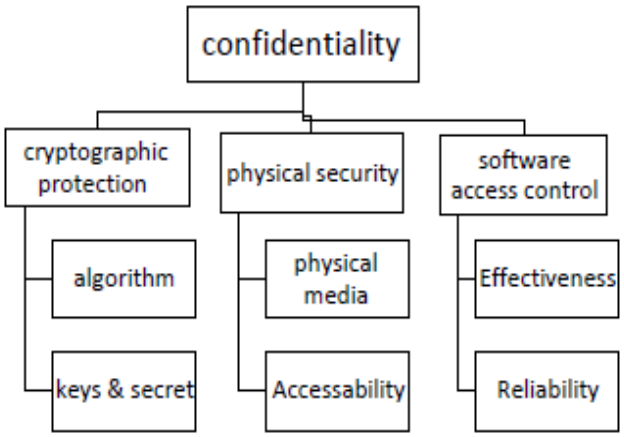

Figure 2: Confidently Model

The integrity model is similar to the one for confidentiality. They both build upon the same key factors which in turn depend on the same lower level criteria. Different questions may be used to assess the criteria in order to reflect unique integrity concerns. Also, in many modern computer systems, authentication is an absolute necessity. Many security services are based on successful authentication. A sample model for authentication is defined in Figure 3. It should be noted that high-level security attributes may also depend on attributes that are not purely security-oriented, such as reliability or predictability, in which case models for these attributes also need to be defined.

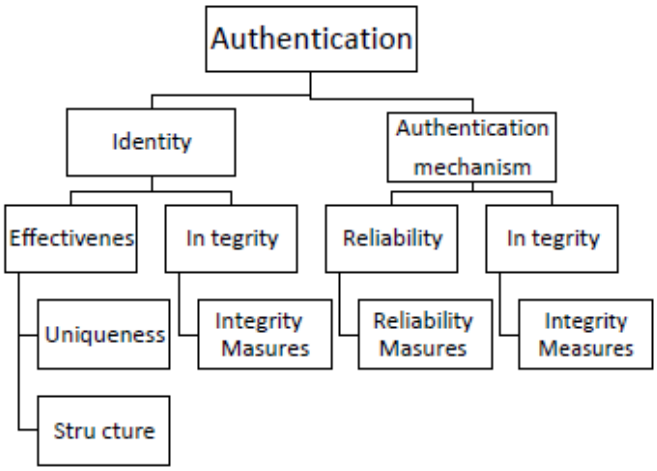

Figure 3: Authentication Model

Software complexity is often hypothesized to be the enemy of software security [12]. The wisdom of security experts is that complexity leads to security problems [10, 6]. The wisdom of these experts, though, has not been substantiated by empirical evidence using quantifiable metrics in terms of software security. However, we cannot control what we cannot measure [11]. Geer [10] also emphasized that a system of security metrics is in the first priority among the tasks for cyber security. Software complexity may be related to security problems or may not. If an empirical relationship can be discovered between software security metrics and security problems at any level (e.g. code, design, or architecture level), these metrics could aid organizations in their efforts to fortify their products early in the development lifecycle.

4. Methodology of SNS

With quick glance on social networking analysis we understand the relation and the information are two main parts which is engaged in privacy. AS we see in figure 4, the independent variables are internet privacy concern, trust in the social networking site, and trust in other members of social networking sites. How do they relate to the outcomes being measured with respect to the use of social networking sites, specifically information sharing and development of new relationships? It demonstrates the privacy trust model.

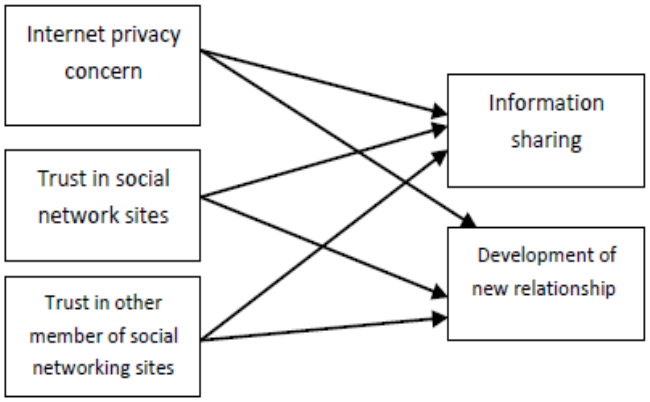

Figure 4: Privacy trust Model

The normal intimacy is depended two main factor, our knowing from the friend it comes from the during the friendship time the second factor is our mutual friends. An ancient proverb said: your friend of your friend is your friend. The histories of friendship maybe make your friend to intimate friend.

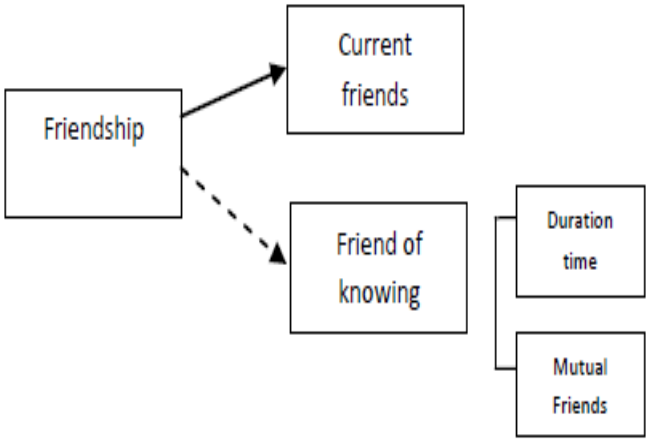

Figure 5: Factors of Friendship

The figure 5 shows the mention factors. The interaction times can embody in social network application like messaging. Duration of knowing can be measured from

adding. The mutual friend plays great role. The number of them shows our level of friendship as result we can decide permit to other friend base of them. We can allow to the friends and FOF to see our profile content base on our measurement .These determination is our cardinal decision to dedicate to everyone a proper level of access to our information. Let's see figure 6:

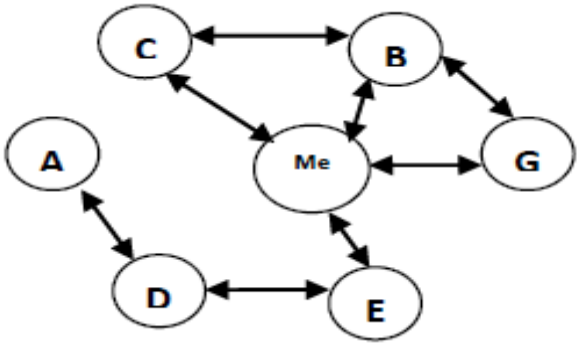

Figure 6: Relationships of Friendship

We observe the relation between 7 nodes it shows ME and B have 2 mutual friend, they are G and C .E is friend of me and vice versa. D id FOF of me and A is FOF of FOF, easily we can depict a privacy layers and assign any node to specific layer. If we put the minimum mutual friend for becoming intimate friend 2 so B is intimate friend is in Intimate layer. The figure 7 shows privacy layer clearly.

Figure 7: privacy layer

This strategy plan to put the nodes (friends) to proper layer by measuring two mentioned factors first mutual friends and secondly time factor which is include inter action times and friendship duration. This work relatively base on your entire number of friends and can develop base on your strategy to participating in new friendship relation whether it is in group or just new friend. The confidant level is value which can put your friend in privacy layer. I prefer the Strategy pattern to adopt and apply more restricted or more benevolent way to dedicate this confidant level value. It is impacted by many different factors from one Social network. It varies dramatically from one social network like Facebook to another. There are three main level of friend which can be assigning to this strategy: intimated friends, close friends and Business friends. In some environments data and documents have sensitivity levels, e.g., secret, confidential. Users have clearances and can access documents based on their clearances. We should consider the main functionality which is being surveyed in mutual friend and theirs trust, Figure 7 shows a Class Model for the Multilevel Security Pattern, it is proper to assign access level of profile content to nodes. In this model users and data are assigned classifications or clearances. Classifications include levels (intimated friends, close friends and Business friends) for confidentiality, access of users to data is based on rules defined by the Bell-LaPadula model [13], while for integrity, and the rules are defined by Biba's model [14].

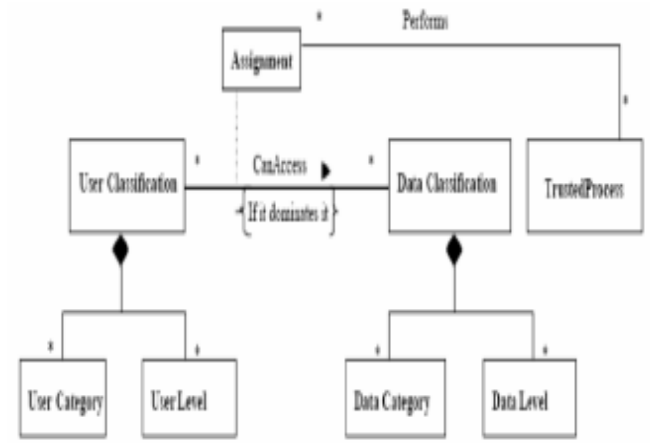

Figure 8: Multilevel Security Pattern

5. Comparison of Security Patterns

Security patterns are a recent development as a way to encapsulate the accumulated knowledge about secure systems design, and security patterns are also intended to be used and understood by developers who are not security professionals. In this section, I will compare two Security patterns to be used when dealing with application security, following an approach that I consider important for measuring the security degree of the patterns, and indicating a fulfillment or not of the properties and attributes common to all security systems. Due to space constraints, I will not consider all the sections of the template but only those sections that we consider relevant to clearly define the considered pattern.

5.1 Authorization Pattern

Intent: It describes who is authorized to access the resources systems.

Context: Any environment where we need to control the access to computing resources.

Problem: The permissions granted for security subjects that have access to protected objects need to be explicitly indicated. On the contrary, any subject could access any resource. Description: To structure the different access policies, we distinguish between active entities (subjects) and passive resources (protection objects).

Solution: The Authorization structure (see Fig. 9) can be captured from classes and relationships or associations.

Consequences: The solution is independent of the resources to be protected. The subjects can be executions of processes, users, roles and group of users; the objects to be protected can be transactions, memory area, I/0 devices, files or other resources of the operating system and the type of access can be reading, writing, execution or methods in higher level objects.

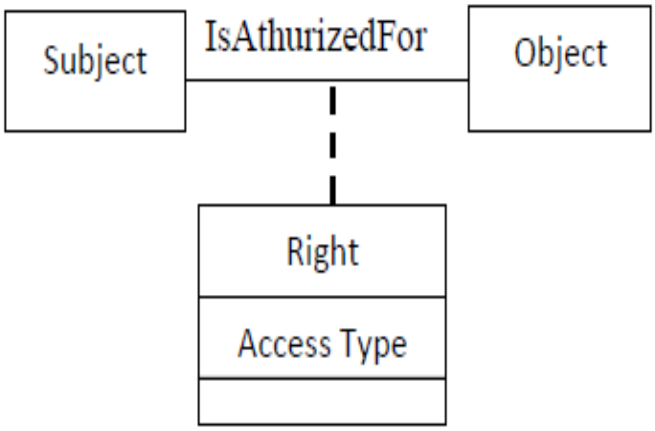

Figure 9: Authorization Pattern.

5.2 Multilevel Security Pattern

Intent: It provides a mechanism of access management in a system with several levels of security classification.

Context: It is applicable to systems that need to provide several security levels.

Problem: How to decide access in an environment with security classifications.

Description: In many systems, data integrity and confidentiality need to be guaranteed. This model would be able to be used in any architecture level and it provides a structure that allows us to have different security levels for both subjects and objects.

Solution: To represent the structure of Multilevel Security, there must be an instance of the class Subject Classification for each subject and an instance of the class Object Classification for each object see Fig. 8. These instances are used to add levels and objects security categories to a subject.

Consequences: It facilitates the administrative work in an environment that requires the classification of subjects and objects. The multilevel security can be expensive since subjects and objects need to be classified into certain levels of sensitiveness.

6. Major attack & malicious use

The access to social networks is commonly done through a web application, so vulnerabilities may be intrinsic to the service. However some attacks seek to overcome the security barriers a web site and explore techniques such as social engineering and trust among users. Each attacker has his own motivations, being interested in specific targets or not, either trying to obtain financial gain or just playing around, but trying to basically obtain and disseminate information of the other users. Below there is a review on the main attacks and malicious use of social networks.

Credentials robbery: Associated directly to identity robbery. In this way, information of users of social networks is used in order to defraud or deceive other users who belong to the same ambience relationship.

Fake Identity: A user employs some means to impersonate another.

Exploitation of Trust: In manual mode, the attacker seeks to enter into a community and behave as a trustworthy user, but it takes some time until all users start to trust this user. In automatic mode, to the attack is based on identity robbery, and using proper tools to diffuse the false idea of a trusted identity.

Bulling and Cyber bulling: Bulling is a form of cruelty in relationships among children and teenagers who are aggressed or harassed in a violent way, making the victims unable to defend themselves. Cyber bulling is similar but without the presence of the aggressor.

Phishing: Capturing information from careless users.

7. Proposed model

Security models seek to find an aggregate structure of protections that allow the improvement of the safety to their users. However the weakest point in the case of a SNS security model would be the user of social networks himself. As a result this model which its idea based on other model suggested by others in (ICOFCS) and I add some modifications and an additions on it which I think it's will be improvement for the model, described after this tries not to transfer or to be based in the user's security system. Given this background, Figure 10 shows a security model that relies on the SNS, thus making them in charge for the security. The model is divided into four phases, which are explained below.

Phase 1

At this phase the model tries to identify the action of automated attack processes, usually known as robots, avoiding that these actions take effect without the need of human interaction, so preventing such attacks. The authenticated user interacts with the system, but it is possible to identify whether it is a human or computer, based on the entropy of this interaction. For this reason, it must be requested that the interaction is analyzed by means of the Turing test. Completely automated public Turing tests are able to distinguish between computers and humans. These tests, commonly shortened to Captcha, in the case they identify the human user if it's a human then allows to this user to access the system, for example Fake Identity.

Phase 2

At this phase it is possible to identify changes in user behavior through activities and other variables that can be mapped and used. If distortions occur about the behavior of the user it might be requested to get user confirmation by

means of positive identification, assuming user has some other secrets, or other information that is only known by the user and assuming that the attacker is unable to know it. However it is necessary to use a second model of authentication and identification (not just user and password). Examples of positive identification such like some private questions like what is the favorite color for you? What is the name of your first teacher? And if the user answers this question correctly, then allow to this user to access the system.

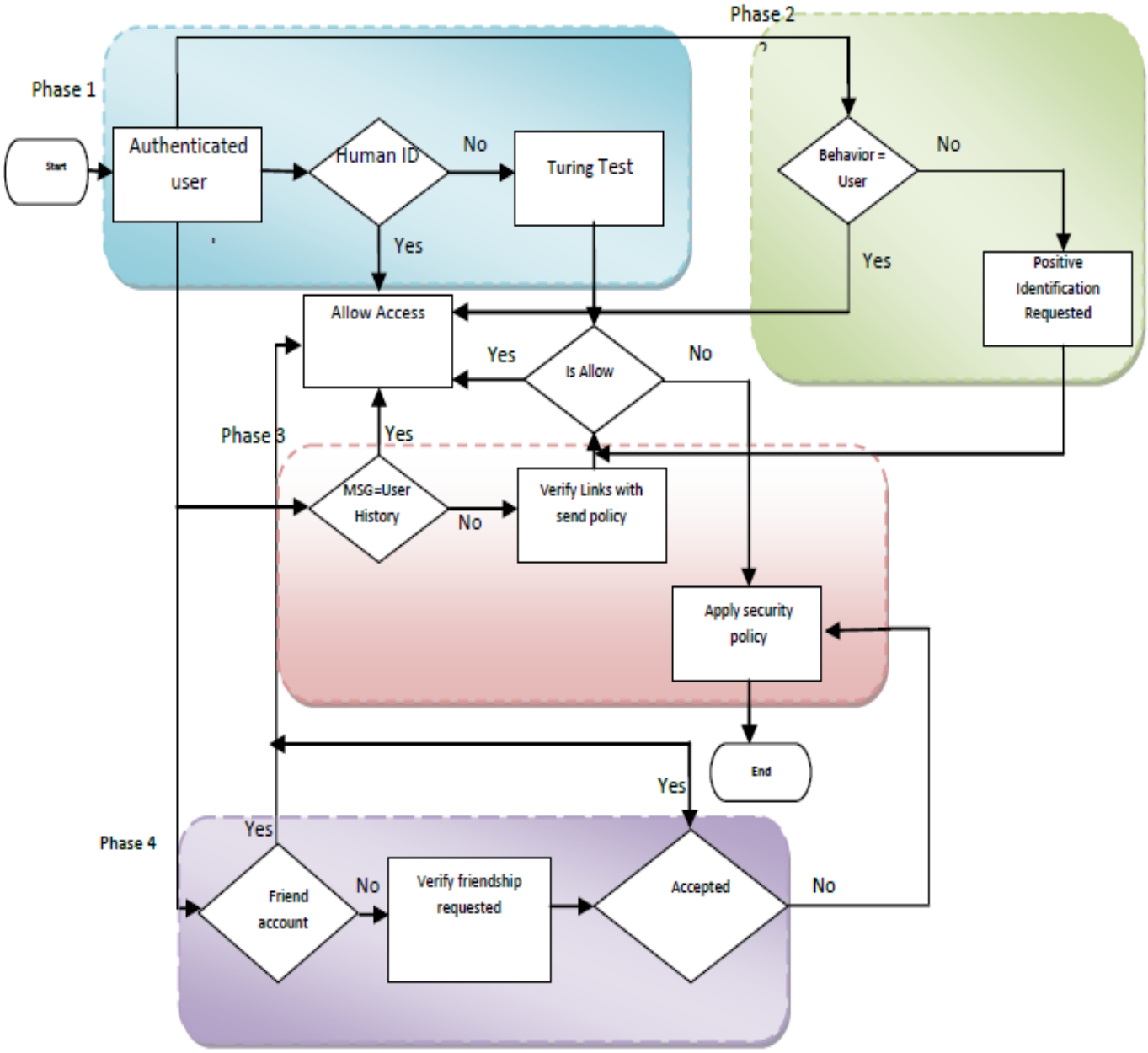

Figure 10: Supposed Model of SNS.

Phase 3

Being a little more complex, this stage can seek to identify the malicious utilization by seemly legitimate users, ghosts (created just to exploit the system), or even other users who have compromised the credentials of other users. In this case, one of the most common attacks would be sending links and information that could be used to trick a user of a trusted community, such like an email from your friend contains a link which is probably damage your computer security. In this case it is necessary to the service provider to establish a policy of minimal use, being necessary to have controls to what can be done and in what amounts it can be done.

Phase 4

At this phase the model tries to identify the action of trying someone to access the user account at social networks applications such Facebook or Twitter and theft his or her profile page and attacking it. To avoid this, the mission of stage is trying to identify the special account of the curious

user who tries to get the other user profile and stalking it. In this case, if the curious user is not one of friends, the model is going to verify the request friendship or the previous added by asking number of questions and tests, to make sure of his or her good intentions. As a result, if it accepted that will allow him to access otherwise, if the utilization policy is violated or even if there is an effort do it, users must have their accounts blocked, from a few minutes to several days, depending on the security policy, or even be banned from the social network community.

Attack	Phase	Security measures
Credentials robbery	1, 2 and 3	Mutual Authentication Model
Fake Identity	1	Data mining Analysis Models
Exploitation of Trust	3 and 4	Model Trust and Reputation
Bulling and Cyberbulling	2 and 3	Data mining Analysis Models
Phishing	1, 2, 3 and 4	-Intrusion Detection System (IDS) and monitoring data from site. - Model Trust

Table I: Summary of attacks and security measures

8. Evaluation

In my opinion, security models depend on how a user deals with his information. In other words, it does not matter how much strong the security is, if the user is careless with his information [15]. Because users employ easily deductive passwords, accept invitations from other users indiscriminately, use public computers with few or no control, click links received in email from strangers, etc., it is very difficult to implement defensive measures. In this model, I embodied the idea discussed by Laerte Peotta de Melo, Edna Dias Canedo, Robson de Oliveira Albuquerque and Rafael Timóteo de Sousa Júnior in THE INTERNATIONAL CONFERENCE ON FORENSIC COMPUTER SCIENCE (ICOFCS) [16]. In this paper I suggested more ensure to allow access the system, also adding four phases to the model to make security model more efficient to remove the security responsibility from the user which I think it didn't mention in previous model. Also a critical success factor for this model is the identification of the incidents in time to be able to avoid or counter the subsequent attack. This consideration requires the model to identify the origin of the attacks and their targets, then allowing identifying the taxonomy of the attack and the attacker's motives.

9. Discussion

How we can give proper level of security and privacy in the social network is it useful. How a user deals with his information. What is main goal of user to joint in social network? How can the providers of social networking services not completely transfer the security responsibilities to their users. Make new friend, share its profile, interesting matter or find new opportunity, they influenced the security somehow to design model which can overcome to misuse of other users.

10. Conclusion and Future work

Social networking has become fully engrained in our societal fabric in a very short time span and turned these networks a nowadays reality for companies that are entering in this environment previously dominated by ordinary users. Thus the security of social networks becomes a critical factor to business, as well as to the common user. I conclude in this paper that considering the attacks that already exist in social networks, there is security measures and metrics intended to improve safety and reduce risks, thus making the environment safer to the users. The model I proposed in this paper has the minimum requirements to address the attacks reviewed and assess the presented defense measures. So in future we can improve this proposed model to be more efficient and implemented it with other technique whose complexity and running time is lesser than the present techniques.

REFERENCES

[1]. A. Acquisti and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the Facebook. Lecture notes in computer science, 4258:36{58, 2006.

[2]. N. Awad and M. Krishnan. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be pro_led online for personalization. MISQuarterly,30(1):13{28, 2006.

[3]. N. Levitt, S. Cheung, "Common Techniques in Fault-Tolerance and Security," Proc. of DCCA 1994.

[4]. C. Meadows, "Applying the dependability paradigm to computer security," Proc. of NSPW 1995.

[5]. E. Jonsson, L. Strömberg, S. Lindskog, "On the functional relation between security and depedability impairments," Proc. of NSPW 1999.

[6]. E. Jonsson, "Towards an integrated conceptual model of security and dependability," Proc. of ARES 2006.

[7]. C. Meadows, J. McLean, "Security and dependability: then and now," Proc. Computer

Security, Dependability and Assurance: From Needs toSolutions, 1998.

[8]. A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, Basic concepts and taxonomy of dependable and secure computing, IEEE Trans. Dependable and Secure Computing, 1(1) 2004.

[9]. SSE-CMM: Systems Security Engineering Capability Maturity gineering Association (ISSEA), referenModel, International Systems Security Enced on July 7, 2008, http://www.ssecmm. org/metric/metric.asp

[10]. Geer, D. E., "A Witness Testimony in the Hearing, Wednesday 25 April 07, entitled Addressing the Nation's Cybersecurity Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action," submitted to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, 2007.

[11]. Fenton, N. E. and Pfleeger, S. L., Software Metrics: A Rigorous and Practical Approach, 1997.

[12]. McGraw, G., Software Security: Building Security In. Boston, NY: Addison-Wesley, 2006.

[13]. McLean, John (1994). "Security Models". Encyclopedia of Software Engineering. 2. New York: John Wiley & Sons, Inc. pp. 1136–1145.

[14]. Biba, K. J. "Integrity Considerations for Secure Computer Systems", MTR-3153, The Mitre Corporation, April 1977. http://man.freebsd.org/mac_biba"Integrity Policies" Power Point presentation from University of Colorado at Colorado Springs

[15]. Centro de atendimento a incidentes de segurança – CAIS/RNP. Segurança em redes sociais: Recomendações Gerais, 2009. Acessível em http://www.rnp.br/_arquivo/disi2009/rnp-disi-2009-cartilha.pdf.

[16]. Donald Steiny, ―Unsocial Networks - Restoring the Social in Social Networks‖. Proceedings of the 42nd Hawaii International Conference on System Sciences - 2009: pp.1-10.