SECUREWALL-A FRAMEWORK FOR FINE-GRAINED PRIVACY CONTROL IN ONLINE SOCIAL NETWORKS

Nadia Razzaq

Department of Computing School of Electrical Engineering and Computer Sciences-NUST, Pakistan
09msccsnrazzaq@seecs.edu.pk

ABSTRACT

Enormous popularity of Social Networking Sites has introduced a great number of privacy risks. Even the most popular of all the social networking sites have characterized access control policies in terms of explicit tracking of the interpersonal relationships between the subjects, objects and their inter relation. In this paper we present a novel paradigm that accounts for a secure, yet sociable information flow model based on access control policies. We took advantage of real time success of the access control security policies in operating systems by implementing them on online social networks at the mandatory level so that the user's privacy does not have to be at stake by the growth of social network and activities or by the level of user understanding of the privacy settings provided by the social networking sites based on discretionary access control. We used Facebook and Google+ as case study and implemented the security policy in SecureWall to mitigate possible privacy leakage scenarios observed. We have implemented Chinese wall policy for community level privacy, Bell la-Padulla access control model to assure confidentiality to the user and Biba Access control model for providing Integrity. Since Bell la-Padulla and Biba models are basically meant to serve military security and therefore can risk sociability, we have combined the two models using Lipner Security Matrix in order to provide security without risking sociability. Our research can be adopted by online social networking sites for the mandatory level security especially for social networking in organizational specific activities.

KEYWORDS

SecureWall, Social Network, Privacy, Mandatory Access Control, Biba, BLP, Chinese wall, Security Model

1. INTRODUCTION

In today's infrastructure, the process of information gathering, processing and disseminating has been profoundly influenced by the emerging popularity of social networking sites. For example, a globally popular social networking site Facebook [3] currently has more than eight hundred million active users. Out of those 50% of the users remain logged on to the website at any given time of the day, about 2 billion pieces of data is shared among them each week, which includes web links, photos, videos, news stories, notes, applications, blog posts etc. These wide opportunities for information sharing and communication keep the social network site popular. This large amount of information sharing on social networking sites, offers some critical challenges to the user information security, as users are willing to reveal private data that is stored in the vast repositories of the social network providers. This private data publication offers many risks to the privacy of a social network user in many possible ways. User might reveal his data accidently due to poor understanding of the default settings of the social network profile, or it might become public through some multi-hop connection for example friends of friend, communities etc.

There is a subtle relation between privacy of social networking sites and their use. Commonly, users of social networks would prefer their personal information to be shared with a small circle of family,

some close friends and not with strangers. Yet few users are still willing to take the risk of revealing some personal information to anonymous strangers. Whatever the case may be private information disclosure can always be of great use to other users, companies groups and third parties, in terms of exploitation. Private information is far more valuable as it can be the data source for marketing, commercial surveys and data mining.

Currently, most of the social network sites have placed the entire responsibility of data privacy to the user alone by providing him with a handful of privacy-setting options that the user has to change as the degree of trust and the friend's connection varies in the dynamic environment of the social network. Besides being a hassle for the user, poor understanding of these settings, also risks the user information privacy. In order to keep sociability and usability intact and yet, provide security to the user information there should be a well-implemented security policy that restricts unauthorized users from accessing the data. This way even if the user accidentally reveals his information, since irrelevant users will not be able to access that information, there will be no risk of data being harvested maliciously. It requires a well-defined access control mechanism to ensure user privacy that must also meet all the challenges offered by the large amount of information sharing and great influx of users in rapidly growing social networks. The access control mechanism should take into account the three types of relationship in social networks i.e. subject-subject, object-object and subject-object. It should also keep into the consideration the dynamic nature of the socially growing network. At the same time, the access control mechanism has to be sufficiently efficient in terms of computation in order to handle the huge volume of access requests. Forthcoming research intends to formulate a security policy to ensure data privacy and to devise a way to implement that security policy for access control in the existing social networks architecture.

The core aim of this research is to propose and implement a security policy that ensures prevention of information leakage on social networking sites through the complex and dynamic connections between users. The approach followed for this research is to develop our own social networking platform to be used as test environment for implementation of the security policies. A controlled environment will be helpful in studying different privacy leakage cases. Chinese wall policy will be implemented for community/groups level security and at the same time, BLP and Biba will be implemented based on labelling strategy in order to ensure confidentiality and integrity, respectively. After implementation of all the security policies, the overall information security will be measured using rate of information flow using entropy and will be compared with the currently popular online social networking sites.

User satisfaction level is also measured qualitative through there feedback on how do they find privacy and integrity in SecureWall as compared to Facebook and Google+. Also how easy it is to ensure privacy in our social network compared to the others. We also took feedback on how much sociability do users think, have been effected through security in comparison to the site that they are already using. It turned out that users gave around 41% feedback in favour of privacy and 37% in favour of user integrity ensured on SecureWall. Sociability results were also up to 29%, along with the ease of settings with a remarkable number that is 43%. Entropy measure also gave satisfactory results of our research. We measured entropy against different scenarios and found out that information leakage in our implementation lies between 3 decimal figures up to 5 decimal figures in different cases which is a lot improved than the entropy of information leaked without our security measures. True alarm rate is in case of information blockage always shows entropy equal to 1.

We divide this paper into six sections; first section is about introduction of the paper. We will discuss the related work, in second part. We will be discussing state of the art policies used by us in this research, in third section. Our proposed approach is explained in fourth section. In fifth section, we will discuss the results and evaluation and last one is about conclusion and future work.

2. RELATED WORK

While surveying the related research work we found that the bulk of existing work focuseson data privacy using encryption based techniques.

2.1. Access Control Using Attributes Based Encryption

With the drastic growth of social networking sites, significant efforts have been made in the field of research to ensure data privacy in social networks. Research emphasis in the past couple of years has been the data privacy at the individual level [2], for example, user preferences, privacy options made available by the social networking sites to their users to hide some data from some users and to show some specific data to others. All these efforts [2], [4], are based on user- awareness about privacy while interacting with the social networking sites or any disclosure of information either intentionally or unintentionally to the third parties who might misuse the information. Yet there are other researchers that do not trust the social networking sites, as there is a clear interest of these sites in disclosing the information to third parties for marketing purposes, for conducting commercial surveys or for data collection. This led them [4],[5],[6] to focus on ensuring confidentiality through encryption. B.Bhattacharjee, and D. Starin [4], present the idea of private social network, which they call Persona. For group communication an attribute-based encryption, PKI, symmetric key and key management is used. User defines groups with arbitrary access to ensure access control over his information. Attribute based encryption keys are used for setting up these groups, assigning the rights and for symmetric key exchange. However it does not address the issue of key revocation in an efficient manner, which is addressed later by P. Mittal, and N.Borisov in [6], using proxy cryptography along with the attribute based encryption technique.

2.2. Information Security on SNS Using Client Side Encryption

M.M. Lucas, and N. Borisov use an encryption-based approach, in [4], a Facebook application named Flybynight. This online social network model is a group based communication approach using client side encryption. They have also used proxy cryptography for group communication. Their approach is to leave only a single encrypted copy of data on Facebook server in order to prevent data mining by the site itself for any means. Using PKI keys and password to encrypt the private key is all a once-only action so it offers usability as well. However, security of that additional password cannot be ensured as it is also entered through the same application. Other than that, this approach only provides encryption to text based objects like messages, status, wall posts etc. but not to the photos, videos, files, notes etc.

2.3. Data privacy by partitioning of information

K. Tang, and P. Francis present another different approach towards data privacy, in [5]. Authors have suggested a substitution cipher named, NOYB. It partitions the user information into atoms and scatters the data by selected transformations. For substituting an information atom with another keeping the logical consistency intact, dictionaries are maintained. This substitution converts the user profile into encrypted form in such a way that not even the host social networking site can detect it. However, a major drawback as a result of this approach is that user profile becomes un-searchable due to this transformations. This makes it almost impossible to search for friends and make new connections for social networking. It removes almost all the possibilities of finding an old friend for social networking. Encryption based techniques do solve the basic privacy problem to some extent, but the problem of trust, remains unresolved. User awareness of a higher level is required for an effective data centric approach. Even for the data-centric approaches to be useful, increased user-awareness is invariably required. Researchers in [1] carried out a detailed survey or user behavior towards the provided privacy options in Facebook. This survey, was carried out two times with a gap of an year and it delineates how frequently users have to change privacy settings on their profile and how much information they exchange online. The survey provides a relation between how frequently

privacy settings are changed, technical knowledge, frequency of use of Facebook, age group etc. The survey also depicts the level of user awareness which has been grown better between the two surveys conducted which could be a reason of media hype about the Facebook privacy problems in United States. It was concluded by the author that privacy risks could be reduced by increasing user awareness and familiarity to privacy options and settings.

Some privacy prototypes [7], had been proposed in the recent past, that focused on information flow model of social networking sites based on profile classification based on suggested prototypes but they all had only been focusing on ensuring individual profile security based on profile view settings. One of the studies has targeted the information misuse through Facebook API's [8], and authors have proposed a privacy-by- proxy design which controls access through hiding that user data from viewers which is not relevant and by using graph anonymization along with identification. Author however, suggests that, this privacy-by-proxy solution is effective only with public user data. Therefore, the private data of the user needs to be submitted by user himself to the application. As a result, applications using user's private data would require users to manually submit this information.

As it is clear that all the studied work are dealing with privacy in social networks, in one way or the other, yet our approach is completely novel in this regard as state of the art security policies have never been implemented in social networks. There have been other policies that were designed by the social network sites themselves but all those policies are discretionary. No mandatory level security is implemented. We are using the policies, which will provide the security according to the requirements of social networking.

3. LEAKAGE CAPACITIES IN SNS INFORMATION FLOW

In the existing social network information model, there exist three sub networks based on the information flow and access control.

- First is the 'information network' that is defined by the relationships among objects (by objects we mean the services availed and the actions performed by the users on a social networking site, for example, status update, private message, photo tag etc).
- Second is the 'social network' which comprises of relationships among subjects (by subject we mean the social network site users).
- Third is the 'inter-network' that is defined by the relationships of the other two networks. Inter-network is the one that defines access control or information leakage.

Every relationship is associated with finite set of relationship types, that is, it can be a friend to friend relationship, it can be an employer to employee relationship or advisor to advisee relationship and so on. Relationship type indicates the interaction of subjects that is, if the subjects belong to the same level or not, which in turn defines the information leakage rate based on the chances that one may share the information to another subject. This is how leakage rate of information is related to the corresponding type of the relationship, that is, if it is a close relationship, higher the rate of information leakage is expected.

Information leakage risk in the existing model is evaluated differently in two different scenarios. One is before the access is given to a subject on an object and the other one is after the access is given to the subject on the object. In Figure 1, the connection between the three networks is shown in the information flow model of the existing social network. The social network N(s) is connected to the information network N(o) through inter-network links, connecting subject s to object o.

Here we can clearly notice that s1 has access to o4 through a friend of friend. The path S1→S2→S3→O3→O4 carries sufficient information of O4 to S1. This is the risk of information leakage before even access is granted. In Figure 1, if the access is granted to S3 on O4 than the relationship type between S3 and S6 is changed to close relationship type that in turn means more risk of information leakage. For example, if a picture O4 is tagged to O3, although it is not owned by S3 yet now it appears to be a part of S3 objects. S1 should not be able to see it but it can be seen through

the path S2 who is a common friend between S1 and S3. This evaluates the risk of information leakage after the access is given to a subject on an object.

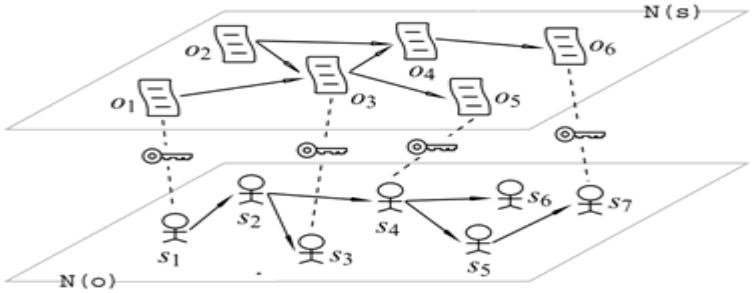

Figure 1. Information Flow Model in Social Networks

4. SECURITY POLICY MODELLING

Modeling a security policy to ensure user's privacy in the information flow of social networking is the main contribution of this research. Any information users post on their profiles can be harvested and used for unethical purposes due to lack of security implementation in information flow as well as the application privacy configuration. Other than lack of awareness to the privacy settings at user level, communities, groups and third party APIs are becoming the major source of exposing user's information to irrelevant and unauthorized viewers. The idea of the proposed research is to implement different type of security policies and information flow models based on profile's classification, to unveil the existing flaws and proposing a solution without making the application unfriendly due to several security checks on the user level. Classification of user profiles will be based on multiple factors that are; user's frequency of usage, user's familiarity to the security tools provided by the social networking site, type of user interaction to the site, width of friend's network, user interaction with communities

Based on this classification privacy settings should be adjusted by the site, without giving the hassle of changing the profile view settings to the user, time and again. This way, chances of information leakage by design will be mitigated to a greater extent, neither in case of any privacy mistake from user nor through the information flow of the site. In the following subsections we will present models of three security polices (1) Chinese wall, (2) Biba and (3) BLP.

4.1 Chinese Wall Policy for Organizational Level Privacy Preferences

Chinese wall policy is a security segment for financial and commercial sector which involves services consultancy. Its basic objective is to prevent that information from flowing which causes conflict of interest among the organization having the same nature of business. Insider information about companies of same work nature presents the potential for employees to abuse company information for personal gain. The best thing about Chinese wall policy is that it has a dynamic approach to deal with this problem. In Chinese wall model, employees, are not restricted to access any kind of information about any company which does not lie under the same conflict of interest class. We apply the same concept for providing security in social networks through controlling information flow and access control.

In this model any type of information, either text based or media based is viewed to be consisting of Objects, o, e.g. in social networking sites (SNS), objects that will be made secure using this model are Profile Information, Wall Status , User Posts , Photo Albums, Videos. Each Object belongs to some Company Dataset, DSyi, where i is a variable for representing different Datasets and y represents the COI class to which that dataset belongs. In SNS it would be related to official pages, closed groups of different Companies that are moderated by the company officials through an administrator.

Companies are further categorized into Conflict of Interest Classes, COIy, where y is a variable to represent different COI classes. Employees belonging to different Companies are known as the Subjects, Si, (where i is a variable that represents the relation of Subject with the Dataset that it belongs to), related to different Company Datasets.Policy rules differ based on the activities performed by Subjects on different Objects belonging to Company Datasets either lying under the same Conflict of Interest Class or a different one, whereas the mandatory rules are generic in implementation. Following are the proposed mandatory rules of the policy:

M-i. S is initially free to choose any DS but once a DS is selected , access to every other DS belonging to the same COI is denied to S.

M-ii. S can read O only if O is in the same DS that is previously chosen by S that is, O is within the wall.

M-iii. S can read O only if O belongs to a COI class whereS has not read any O , i.e. O is outside the wall.

M-iv. S can write O only if clauses (M-ii) & (M-iii) are held true for read access to O by S.

M-v. S can write O only if no object can be read which lies in a different dataset to the one for which S has requested thewrite access which also contains un-sanitized information. It implies that the flow of un-sanitized information is confined to its own dataset. Sanitized information however can flow throughout the system.

In order to implement the Sanitization concept on social networking, a database of policy phrases of sensitive information is to be compiled by the Company Dataset Administrator as per the company security policy at the time of group creation. These phrases are checked at the time of posting by a policy bound member, that is the one who have viewed or posted unsanitized information on a dataset wall in one COI and is now bound with this dataset for not leaking any private information to other datasets within the same COI by one way or another. Discretionary rules of the Chinese wall policy for social networking are based on the response of the security model to the individual actions by Subject on Object.

For explaining these policy rules we take an example of a class that includes all the banks. Since all the banks have the same nature of work therefore all the groups and the pages of the banks lie under the same Conflict of interest class , say , COI_b. We suppose that there is another class that has all the oil companies in its dataset, COI_o.

Dataset DS_{b1} , DS_{b2} , DS_{b3} belongs to COI_b i.e.

$$A_{banks} \in COI_b \text{ such that } A_{banks} = \{ DS_{b1} , DS_{b2} , DS_{b3} \ldots \}$$

Whereas, Dataset DS_{o1} , DS_{o2} , DS_{o3} belongs to COI_o i.e.

$$B_{oil} \in COI_o \text{ such that } B_{oil} = \{ DS_{o1} , DS_{o2} , DS_{o3} \ldots \}$$

We assume that E_b is a proper set containing friend lists of all the datasets belonging to COI_b i.e.

$$E_b = \{\text{Members of } DS_{b1}, DS_{b2}, DS_{b3} \ldots .\}$$

When a Subject S sends a request to join a group or a page of DS_{b1}, DS_{b1} will check every possible previous connection of S with COI_b up to three levels. We represent it with a set Sf = { S , friends of S (F) , Friends of Friends of S (fof)}. If any connection of S is found with a DS_b such that it belongs to COI_b but not DS_{b1} i.e.

$$E_b \cap S_f = x \text{ where } x \in COI_b \mid x \in DS_{b1}$$

then the request will be denied by DS_{b1}. If no connection is found i.e. $E_b \cap S_f = \{\emptyset\}$, or a connection is found only with DS_b then membership will be granted to S.

Once the access is granted to S we will call the subject as S_{b1} as it belongs to DS_{b1}. S_{b1} can now read and write any object that belongs to DS_{b1}. S_{b1} can post anything on the DS_{b1} page or group, can comment on other's posts on the DS_{b1} page or group, can tag pictures, videos or URLs to any other Subject that belongs to DS_{b1}. S_{b1} cannot post any Media type Object across the wall. This is for the

fact that Media type objects cannot be scrutinized based on database matching approach and therefore it needs human intervention at a frequent level that might reduce the usability. Since in social networking usability and sociability cannot compromise hence we reserve the media type Information flow across the wall.

While allowing a subject to let the information flow across the wall it has to be ensured that only Sanitized information should flow. To ensure this group or page administrator /moderator of every dataset will be providing the application with a set of phrases that if found in any post, it is not considered safe for posting outside the wall. Such posts will be sent to the moderator of the Dataset to whom subject belongs, if it is approved by the moderator only then it will be posted on any other Dataset from a different COI. It is also made sure that no subject can read more than one Dataset in a COI(as mentioned in Scenario-6). Following are the detailed scenarios of policy for implementing Chinese wall on social networking site.

Scenario 1. S_i sends a request to join a DS_{b1} then access will be granted only if ;
Either,

$$Eb \cap Sf = \{\emptyset\} \quad (4.1)$$

Or

$$Eb \cap Sf = x \quad (4.2)$$

Where,

$$x \in COIb \mid x \in DSb1 \mid x \notin \{Abanks - DSb1\}$$

Access will not be granted if;

$$Eb \cap Sf = x$$

Where,

$$x \in COIb \mid x \notin DSb1$$

Scenario 2. DSb1 administrator must compile a database of policy statement , set K, about the confidential information which should not flow beyond the wall i.e. un-sanitized information.

Scenario 3. Once approved i.e. Sb1∈DSb1, Sb1 can read any Object O, as long as O ∈DSb1.

Scenario 4. Sb1 can write any Object O, as long as O ∈DSb1 that is un-sanitized Information flows within the wall.

Scenario 5. Sb1 cannot read any Object such that,

$$O \in COIb \mid O \in \{Abanks - DSb1\} \quad (4.3)$$

Scenario 6. Sb1 can read any Object such that $O \notin COIb \mid O \in COIo \mid O \in DSo1$ only if ;
Either,

$$Boil \cap Sb1 = \{\emptyset\} \quad (4.4.1)$$

Or,

$$Boil \cap Sb1 = x \quad (4.4.2)$$

Where,

$$x \in COIo \mid x \in DSo1 \mid x \notin \{Boil – DSo1\}$$

Sb1 cannot read any object such that $O \notin COIb \mid O \in COIo$ if;

$$Boil \cap S\ b1 = x \text{ where } x \in COIo \mid x \notin DSo1 \quad (4.5)$$

Scenario 7. Sb1 cannot write any Object such that

$$O \in COIb \mid O \in \{Abanks - DSb1\} \quad (4.6)$$

Scenario 8. Sb1 can write an Object such that $O \notin COIb \mid O \in COIo \mid O \in DSo1$, if and only if all the following points are held valid i.e.

- Condition in Scenario 6 is held true.
- Object type is Text not Media.
- $\cap K = \{\emptyset\}$ i.e. Object must not have any word that belongs to set of phrases specified by DSb1.

Scenario 9. If Sb1 tries to post a comment on a Dataset, DSo1 such that $O \cap K \neq \{\emptyset\}$, the post will not be posted on DSo1 and will be send to moderator of DSo1 for approval or rejection along

with the comments.Sb1 will be notified of pending post for the reason of containing inappropriate content .

Scenario 10. In Scenario- 9, Object will be posted on DSo1 only if moderator DSo1 approves the object for posting. So1 will be notified. Object will not be posted on DSo1 if moderator DSo1 rejects the object for posting and sends the post back to So1 for revision and removal of the security violating content. This way only Sanitized information will flow across the wall.

Scenario 11. Every time a new group or page is accessed by the Subject, condition in Scenario-1 will be checked

If ,

$$Eb \cap Sf = x \text{ where } x \in COIb \mid x \notin DSb1 \quad (4.7)$$

(where S_f in this case comprises of friends and friends of friends) holds true at any stage , Subject will be intimated for the possible information leakage threat and sanitation check will be activated on S_b profile.

As mentioned in Scenario- 11, Sanitized information will move across the wall , this way neither we will bound the Subject with reduced usability nor will any information be exposed to any other COI that may be readable to any subject belonging to a dataset of their own conflict of interest class. This is how Chinese wall policy is implemented on a social networking site without compromising security or usability.

4.2 BLP and Biba Security Model for User Level Privacy Preferences

BLP model and Biba model both were basically proposed to serve military security requirements which made the two models unable to coexist at the same time in the same system where as in order to ensure security in commercial or non military systems, confidentially and integrity can be required side by side, so there has to be a way for the two models to coexist. We combined the two models for simultaneous implementation using the same controls by remapping of the labels based on dominance relation inversion.

BLP model was motivated by the confidentiality requirement where as Biba was designed for integrity purposes but the controls used for both the models were same. This makes the Biba rules to be duals of corresponding rules in BPL. It has not been specified by any rule whether to place high integrity at the top of the lattice or to place high confidentiality at the top of the lattice, besides top and bottom are the relative terms and not rules specified. We used this point to bring information flow in Biba model in line to the BLP model by placing low integrity at the top of the lattice along with the High confidentiality and vice versa. All it changes is that it inverts the dominance relation that is low integrity to be dominant to the high integrity. The Lattices drawn as a result of the two models are shown in Figure 2 and Figure 3. These lattices decide the sensitivity or confidentiality and the integrity dominance of subjects and objects but then comes the problem of calculating the access rights based on the dominance relation defined by the combined model of Biba and BLP labels. For this matter we used Lipner matrix. Lipner gave the detailed matrix for calculating the access rights of subjects on objects by giving an example of a commercial system.

In order to create Lipner matrix, let us define the subjects, objects, their sensitivity and integrity categories and levels.

4.2.1 Subjects

Subjects are categorized based on the closeness of relation to the owner profile. It is divided into four categories namely, “Family”, “Friends”, “Colleagues”, and “Acquaintances”.

4.2.2 Object

Objects are taken to be all the basic ingredients of SNS that holds a chance of information leakage. Objects under our analysis are; “Wall”, “Posts”, “Albums», “Activities”, “Friend-list”, “Applications”, “Pages”, “Groups” and “Profile Information”.

4.2.3 Sensitivity Level (λ)

Four sensitivity levels are as following;

Personal: (λT) It is the top level security. Information on this level, can only be shared to the trusted ones

Informal: (λH) It is the second level of security or can be called high level security. Close friends may access information on this level.

Formal: (λM) It is the third/medium level security. Information on this level, may be accessed by colleagues

Open: (λL) It is the low level security. Information on this level, can be viewed by all the friends

4.2.4 Sensitivity Category (λcategory)

Objects are divided into categories based on the sensitivity of information content from privacy aspect.

Private Content: Private content is a category of objects which includes DOB, location, education, work location, relationships, friend-lists

Groups Content: This category includes user's posts activity on the groups he has joined.

Third party Content: All the content that is posted on one's wall by third party API's, games and promotions and updates from Pages are included in this category.

Activities: This category comprises of user activities like status, likes, comments on other's post, tags, friend-requests, joining of a group or page or application.

Postings: This category comprises of wall posts, friends shared posts, pictures, albums by the owner

4.2.5 Integrity Level (Ω)

Here an important point needs to be cleared before we get in to the details of access rights, that is, labels here are named soonly for convenience to elaborate high or low integrity. It should not be confused with the access rights as "write" or "read" with "view", "comment "or "share"

Share: (ΩH) This is high level security as the subscript "H" shows it. Subject at this level is the most trusted and have the right of viewing the post, sharing the post further, viewing comments and writing comments

View Comment: (ΩM) This is the medium integrity level. Subject at this level belongs to trusted category (which might be source of reliable information as well) and have the right of viewing post, adding comments, viewing comments but cannot share.

View: (ΩL) This is the low integrity level. Subject at this level is lowly trusted and only has the right of viewing the post. He cannot view comments or add comments and cannot share the post further.

4.2.6 Integrity Category (Ωcategory)

Integrity categories are divided based on the fact that how often the information varies and are these variations from the owner (trusted) or from others.

Invariant: It includes information, which is not changed frequently for example profile information, friend-list and groups

Variant: It includes information, which changes frequently for example wall postings, albums, Third-Party content

Variation Log: It is the type of content, which is regarding user activities for example, posts regarding user activity on a group or user joining a page etc. that appears on the wall and is visible publically in case of other social networks without intervention of the user himself.

4.2.7 Security Clearance and Classification

Everything under the category "Posting" will have a label assigned by the owner at the time of posting the content and that is why it will only be considered as a relative term for every subject. The details of security labels of individual postings will be discussed in section 4.2.8 and 4.2.9. Since group

information is also not supposed to be shown to any one therefore we merge the security category "Group" into "Private Content".

4.2.8 Sensitivity and Integrity Clearance of Subjects

Table 1 shows clearly the sensitivity clearance and integrity clearance of every Subject which explains the position or level of the subject in BLP lattice and Biba lattice respectively.

Table 1. Sensitivity & Integrity Clearance of Subjects

Subjects	**Sensitivity Clearance**	**Integrity Clearance**
Family	Personal {Private Content , Postings}	Share {variant} view{invariant, variation Log}
Friends	Informal {Postings, Third-Party, Activities}	Share {Variants} , View {Variation log}
Colleagues	Formal {Postings, Third-Party, Activities}	View Comment {Variants}, View {Variation log}
Acquaintances	Open { Postings, Third-Party }	View {Variants}

4.2.9 Sensitivity & Integrity Classification of Objects

Table 2 shows the sensitivity classification and integrity classification of every Object which explains the security level of the Object in BLP lattice and Biba lattice respectively.

Table 2. Sensitivity & Integrity Classification of Objects

Objects	**Sensitivity Classification**	**Integrity Classification**
Wall	Personal (Postings)	View (Variants)
	Informal(Postings)	
	Formal (Postings)	
	Open (Postings)	
Posts	Personal (Postings)	Share (Variant)
	Informal(Postings)	Share (Variant)
	Formal (Postings)	Share (Variant)
	Open (Postings)	View Comment (Variant)
Albums	Personal (Postings)	View Comment (Variants)
	Informal(Postings)	
	Formal (Postings)	
	Open (Postings)	
Activities	Informal(Activities)	ViewComments(Variation log)
Friend-list	Personal(ϕ)	Share (Invariant)
Applications	Informal(Third-Party)	View (Variants)
Pages	Informal(Third-Party)	View (Variants)
Groups	Personal(ϕ)	Share (Invariant)
Profile Information	Personal(Private Content)	Share (Invariant)

4.2.10 Dominance Calculation according to the lattice

Since each of security clearance and classification in our case has two labels, a confidentiality label, having BLP mandatory control and an integrity label, having Biba mandatory controls. Biba lattice

Figure 2. BIBA Lattice-downward flow

Figure 3. BLP Lattice- upward flow

shown in Figure 2, applies the rule with only downward flow allowed.
Figure 3 shows the BLP Lattice following the rule of upward flow allowed.

Combined mandatory controls will be

- Subject s can read Object o only if;

$$\lambda(s) \geq \lambda(o) \quad \& \quad \Omega(s) \leq \Omega(o) \tag{4.8}$$

- Subject s can read Object o only if;

$$\lambda(s) \leq \lambda(o) \quad \& \quad \Omega(s) \geq \Omega(o) \tag{4.9}$$

For dominance of course Need-To-Know rule is also required to be fulfilled other than these two rules i-e.

- Subject can only access (read/write) an object if;

$$\lambda_{category}\ \Omega_{category}\ (s) \subseteq \lambda_{category}\ \Omega_{category}\ (o) \tag{4.10}$$

As our model needs the simultaneous implementation of the two lattices for BLP and BIBA so in order to keep the direction of controls the same, we need to invert the matrix .It will provide us with mathematically one lattice which in turn is a product of two lattices i-e BLP lattice and BIBA lattice.
Let Λ be the set of Confidentiality Labels and ω be the set of Integrity labels.

$$\Lambda=\{\lambda_T,\lambda_H,\lambda_M,\lambda_L\} \tag{4.11}$$

Where, levels are arranged in the following order, $\lambda_H \geq \lambda_L$

$$\omega=\{\Omega_H,\Omega_M,\Omega_L\} \tag{4.12}$$

Where, levels are arranged in the following order, $\Omega_H \geq \Omega_L$
Dominance relation calculated based on the rules mentioned above will assign the read/ write access based on the following matrix, provided 'Need to Know' rule is fulfilled. In the matrix we will be using high and low as a general term and by high, we mean any security level higher than the security level in comparison at that time which can be Top security level, high security level, medium security level, or low security level as mentioned in equation 4.11 and 4.12.

Table 3. Access Calculation in Privacy lattice

	Objects Classification				
Subject Clearance		$\lambda_L\Omega_L$	$\lambda_L\Omega_H$	$\lambda_H\Omega_L$	$\lambda_H\Omega_H$
	$\lambda_L\Omega_L$	rw	r	w	ϕ
	$\lambda_L\Omega_H$	w	rw	w	w
	$\lambda_H\Omega_L$	r	r	rw	r
	$\lambda_H\Omega_H$	ϕ	r	w	rw

In Table 3 each entry shows the maximum access that a subject, labeled in row can have on object, labeled in columns by combining the two lattices. Let's discuss a scenario of access right based on the classification and clearance assigned in Table 1 and Table 2.

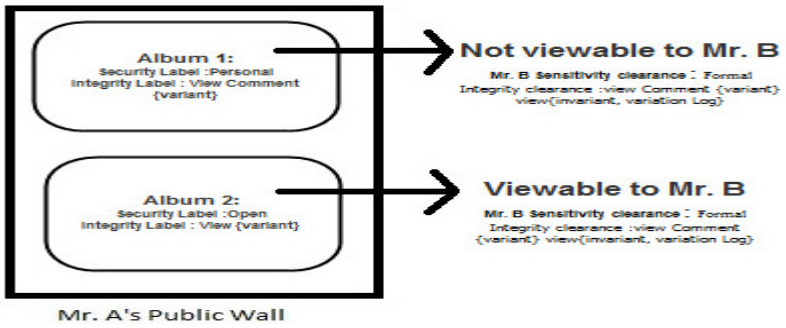

Figure 4. Access based on Security Classification of object and Security Clearance of subject

Suppose owner of the wall say X has labeled his wall security as Informal {Postings} λH. System has set the integrity of wall as View(variant) ΩL. If a subject from the category Family tries to post something on the wall who has a sensitivity clearance as Personal (Private Content, Postings) λH and integrity clearance as Share {Variant} ΩH.This makes subject clearance as λHΩH and object classification as λHΩL whereas from Table 3 we see that this Subject has write access to the wall. Similarly, in Figure 4, it is clearly shown that Mr. B cannot view Album1, as the security and integrity classification of the object Album1, is higher than the security and integrity clearance of B. Album 2 on the other hand, is viewable by Mr. B because security and integrity clearance of B is higher than the security and integrity classification of the object Album 2.

5. IMPLEMENTATION

For our implementation we have used an open source platform named Oxwall[20], which is designed as a plugin based online network framework so that for any further developments it may provide enough room to meet desired requirement, yet it has its own set of limitations based on the defined rules to meet our security needs. Developing a whole new framework is no doubt a tedious job so the question arises why did not we use existing social networks like Facebook or Linked-in as these both provide with "Developer Application" facility. The answer to this very relevant question is that the scope of our research was only to be achieved by implementing an upper layer of the available interface as we had to implement mandatory access control and not discretionary access controls. Existing social networks do provide discretionary access controls to their users. A developer application of course does not have the access to the social network framework, which is an essential requirement for enforcing security access controls at the mandatory level. This reason alone, rules out any possibility of using existing online social networks. Other than that even if developer applications had the access to the online social network framework, there is a lot of limitations imposed by the social networks policy that abstain to practice any application which overrules their existing privacy settings.

5.1 Platform Architecture

Let's begin with an overview of the platform used for SecureWall[24]. Basic framework sticks to the same concept of every social networking web framework that is triangular model-view-controller (MVC) architecture. In this architecture "View" directly updates "Controller" which then updates "Model" and then "Model" updates "View" directly. Controller and View both are loosely dependent on data-tier and service layer. Controller in our application is the main functional worker as it keeps all the routed requests. It fetches user input, communicates with Model and provides the data for the purpose of rendering View. Business logic implementation and interaction with databases is the responsibility of Model. Model includes two instances, first, service that is responsible for business logic and second, data access object that controls manipulation of databases. As for View, it is

responsible for presentation logic. It receives processed data which is ready for markup which in our case is represented by HTML template supported by Smarty Logic.

In our architecture, managers are represented in terms of global objects for main functionality and are accessed by a special static class. Basic SecureWall core provides simple community features that can be found in any other social networking software that is, friends networking through requesting, adding or removing friends, user profile creation and content management, built in search engine optimization using slugs uploading and sharing of contents etc. In the application most of the objects are built as singletons that is global objects for example all the managers, data access objects, service objects, this makes these objects accessible through out the package for any implementation. It requires a web server which is capable of running PHP 5.2.6, Apache 2 and MySQL 5.0 at lower bound. For Oxwall it is preferred that Ampps 1.0 is used for local server. "PHP 5.2.6" is used as the programming language, JavaScript, HTML and CSS is used mostly for views. Template engine "Smarty" is used for compiling customizable templates rather than using native PHP templates which are not customizable graphically.

5.2 Implementation Challenges

Matrix formation and access calculation based on the level of distance from the user also has an extensive implementation but controlling information flow through a group was a bigger challenge than controlling access control on user's profile, as members of a group are not friends to each other. Also groups usually contains information that targets masses, sometimes including random public. Users who are registered with only one group in a COI, is allowed to access un-sanitized information of the group which is the unfiltered sensitive information of that group. User ID of such a user is entered in that table "sanit" along with the COI information. Whenever he tries to view or post un-sanitized information on a group, his prior affiliation with respective COI is verified. As it can be seen in Figure 5, that when a user is found already affiliated with any other group in the same COI, used as 'cat', "sanity_violation" error is thrown and user access request to un-sanitized information is denied. User is shown the error alert that he cannot access un-sanitized information of this group as he is already policy bound with another group in the same COI.

```
$res1 = mysql_query("SELECT category, title FROM ow_groups_group  WHERE id = $grpId", $con);
        $row_grp = mysql_fetch_array($res1);
        $cat = $row_grp['category'];
        $groupName = $row_grp['title'];
$res = mysql_query("SELECT distinct val, group_id, category FROM sanit WHERE user_id = '$userId'
AND category = '$cat' AND val = '0'", $con);
        $row_count=mysql_num_rows($res);
                if($row_count>0)
                        row_grp1 = mysql_fetch_array($res);
                else
                        $row_grp1['group_id']=$grpId;
                if($_POST['sanitized'] == 'yes' && $row_grp1['group_id']!=$grpId)
                {
                        echo json_encode("sanity_violation");
                exit;
                }
```

Figure 5. Shows how un-sanitized information is prevented from getting leaked

This user is not bothered with any error or alert on this group if he posts or reads sanitized information. Similarly if he was not bound with any group in the same COI previously, than he would be granted access to the un-sanitized information and he will remain policy bound with this group.

As mentioned earlier in section 4.1 group's privacy policy statements are defined at the time of creation of group. This set of statements is saved in database along with the set of n-grams for every statement, Figure 6. When a policy bound user tries to post some information n-grams from his texts are calculated on send button click and are compared with the initially calculated n-grams of the policy to calculate the percentage of amount of similar information. If the percentage exceeds the threshold,

```
$sql = "select ngram,percent from ow_knowledge_base where group_id = '$grpId' && ngram in
('".implode("','",$info)."')";
                $r = mysql_query($sql,$con);
                $knowledge=array();
                while ( $row = mysql_fetch_array($r) )
                        {
                                $knowledge[ $row['ngram'] ]  = $row['percent'];
                        }
                foreach($ngrams as $k => $v)
                        {
                                if ( isset($knowledge[$k]) )
                                        {
                                                $acc += $knowledge[$k] * $v;
                                                $total++;
                                        }
                        }
                                        $percent = ($acc/$total)*100;
```

Figure 6. Shows how n-grams are used to ensure group policy

which in our case is set to 45%, that text is not posted and user is shown a message regarding policy violation. N-gram percentage check is applied on every post made by a policy bound user. His post might be on that group, any other group within COI or outside the COI, on its own profile, on friend's wall, on a page or anywhere on the social network that might carry the risk of group information leakage.

6. RESULTS

For the results, we followed two approaches, first using evaluation of SecureWall in comparison to the existing sites and most popular online social networking sites i-e Facebook and Google+, second we used entropy for measuring the flow of information at different level of closeness of relationship.

6.1 Evaluation

We created an evaluation form for this purpose which contained twenty questions in total to get the view from the users regarding, (1) which OSN provides effective privacy, (2) how easy it is to use our social networking site as compared to the other one that they are already using, (3) how less they have to worry about their privacy in our site and, (4) how sociable is SecureWall compared to others. We gathered data from over 266 users and had them fill the form, which is available in Feedback section of SecureWall. Our evaluation has given us some good figures on user's satisfaction ratio among SecureWall and the most widely used social networking sites, Facebook and Google +. For evaluation, we presented five options to the users for showing their satisfaction, starting from very high to none at all, for all the three OSNs. Figure 7, for instance shows the evaluation results we got for the post privacy. Out of 266 users who gave their feedback 5% users marked post privacy of SecureWall as very high, 7% users marked it Low, 28% users think its high and 24% users marked it as medium. It can be observed clearly that user post privacy in Facebook is also liked by many users. We got the feedback for almost all the aspects that are thought to be a part of social networking site in terms of privacy, integrity, sociability and usability. In privacy it further catered to areas for instance individual level privacy, group level privacy , profile exposure, friend's profile exposure , pictures privacy , posts privacy , user activities privacy etc. Figure 8 shows the overall feedback that we received for the three sites, in terms of privacy and the above mentioned

factors y-axis in evaluation graphs shows the percentage of users evaluating the properties mentioned at x-axis. We can see that individual level privacy is marked with no significant difference between Facebook and SecureWall, but at the same time, it can be observed that group privacy provided in SecureWall is something clearly missed in the other two. Similarly profile exposure and activities privacy in SecureWall is also marked significantly high.

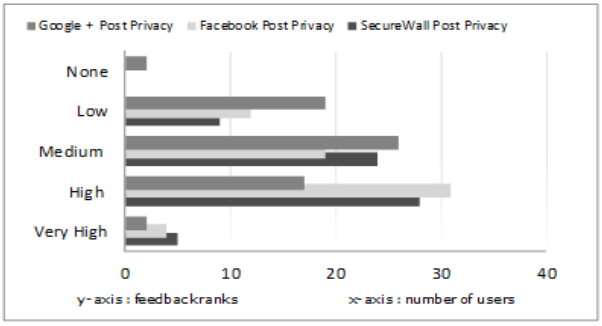

Figure 7. User Satisfaction Graph for Post Privacy

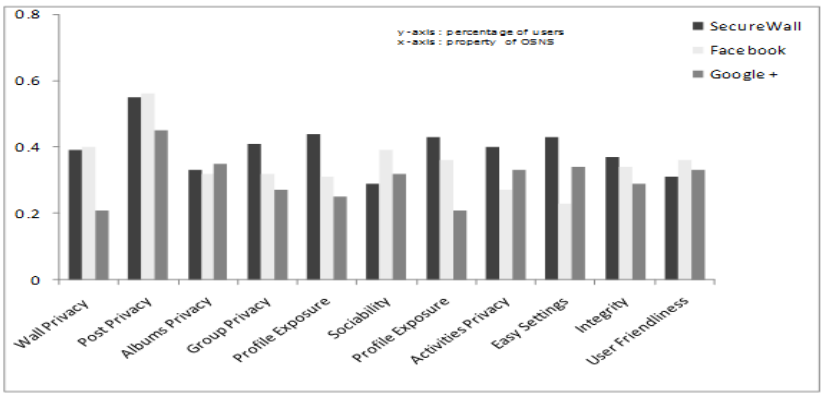

Figure 8. Evaluation Results Based on User Feedback

Apart from security, integrity of the information that reached the user, has also been marked better as compared to Facebook and Google +.

Overall ratio of the given social networking sites for integrity of information and for all the aspects of privacy in combination, are shown in Figure 9 and Figure 10 respectively.

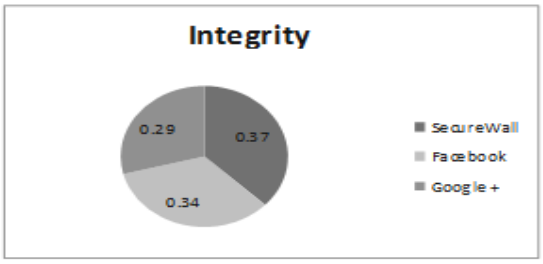

Figure 9. Integrity of Information

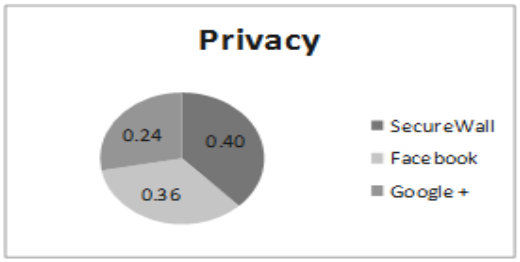

Figure 10. Privacy Ratio

Despite the good statistics found for privacy and integrity, in user's feedback, we do notice the difference marked in sociability and user friendliness for SecureWall compared to Facebook. In our point of view the major aspect for this difference in user friendliness can be that SecureWall has been experienced by the users for the first time whereas Facebook [22] has approximately 7012.9 million visits per month and is established for over 8 years now, which justifies the aspect of user's acclimated friendliness of the site.

This argument can also be supported by the fact that Google + is also not considered as user friendly as Facebook for the very reason explained by the demographics given in [20].

As for sociability, as it is a well-known fact that security always comes with restrictions and boundaries which of course in case of social networking are not greatly appreciated. Compared to Google+ difference for the sociability graph is not that significant. At the same time, we may notice a remarkable raise of graph for SecureWall for the ease of privacy settings. Obviously it's the mandatory access control mechanism, which compared to the Facebook and Google+, is a lot more convenient, user has to worry the least about the privacy settings, and yet he remains confident about his privacy. This happens to be the crux of the whole research as none of the social networking sites has any mandatory access control mechanism, they all follow the discretionary access control where each object's privacy needs to be set explicitly and yet it leaves a chance for privacy leakage specially where user is new or naïve. Figure 11 and Figure 12 depict the clear picture of ease of settings ratio and sociability, respectively, among the three sites.

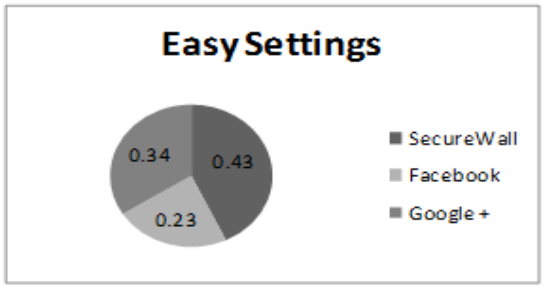

Figure 11. Level of Ease for Privacy settings

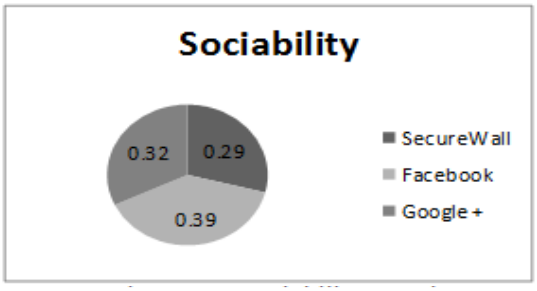

Figure 12. Sociability Graph

6.2 Measure of Information

An information-measuring tool was required to find out where have we blocked the sensitive information flow and where has it given the rightful access to the information. Since we couldn't find any information-measuring tool already available, therefore, we designed an entropy calculator and implemented it in C# Dot Net. It takes either HTML or TXT file as input. We can also add the words and phrases that are to be excluded from entropy measure. These can be such words or phrases which usually are used in English but are not considered to be having any information in it e.g. the articles, [23].

For calculating the number of times a forbidden or policy phrase is used, we simply used search page functionality. It was useful in measuring the count of the phrases that were used in policy defined for any group in COI. If the word from forbidden phrase are found and is not alarmed, we check its context. Let the forbidden phrase from the policy of a group belonging to COI¬a, be P¬DSa1 and any word belonging from that phrase be WDSa1, and then the count of the first word belonging to P¬DSa1 will be WnDSa1where N is the total number of words from phrase. We first find such words, then compare their context with the policy and if found similar then we count such words and apply the Shannon's Entropy formula in the following way [21].

$$\text{Entropy of Phrase} = \begin{cases} -\sum_{n=1}^{N} \frac{W^{n}_{DSa1}}{W_{DSa1}} \log\left(\frac{W^{n}_{DSa1}}{W_{DSa1}}\right) & \text{if Words found} > 0 \\ \text{if Words found} = 0 \end{cases} \qquad \text{.....(4.13)}$$

where n is number of words found and N is total number of words.

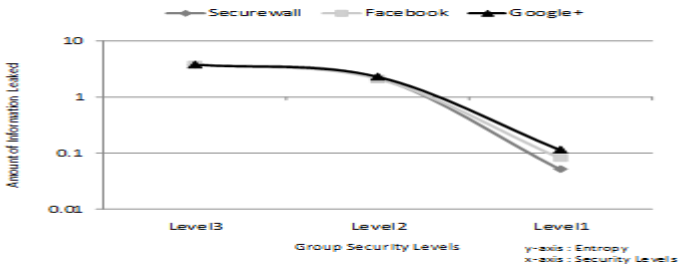

Figure 13. Sensitive Information Moved within Same COI

We calculated entropy for different case scenarios, shown in Figure 13. To find out how much of the information have we stopped from flowing across the wall within same COI, we created the same groups on Facebook, Google+ and on SecureWall. Since there is no concept of policy phrases in Facebook and Google+, so its flow from one group to another is 100%.The only privacy that could be found in Facebook at group level was to either mark it as "Close group" or "Secret group". Secret groups are only known and joined by those to whom administrator sends the invitation whereas for close groups, everyone can send the join request yet only the ones approved by administrator becomes the member. In both the cases content can be viewed and posted by members only. Here we observe that copying of content by a member and posting it to any other group, which may be aligned to the same class of interest, is not checked at all. Therefore, organizational level social networking has no privacy assured at any of the existing social networking sites. Even if the organization owns one of its own social-network within the organization, it has to make it role based, and the administrator has to watch over the permissions of every role explicitly. Although private social networks are not in focus for this research, yet our research can be used for this purpose without the hassle of role management, but we are not going to discuss it here for the obvious reasons. Before we give details of the case scenarios let us take a look at the example of how information will be blocked in a group and that blocked information will have its own entropy which will be used for true alarms case scenario as explained in case 5.

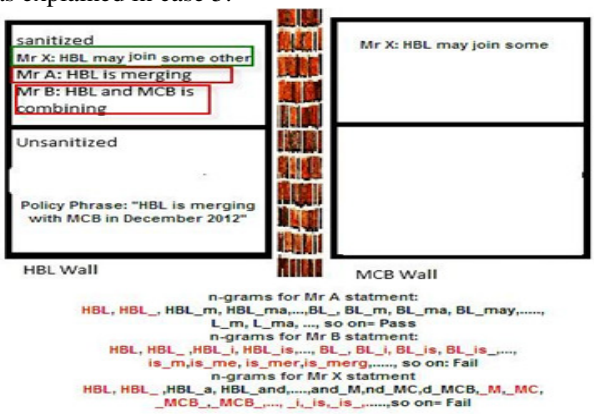

Figure 14. Example of Information Blocked Based on N-gram Match

Here we took an example of two datasets within the same COI, HBL and MCB. Information in the un-sanitized part of the wall can bear the complete policy phrase as it is but in sanitized wall it has to be filtered before posting. In Figure 14, statement of Mr. A and Mr. B cannot be posted due to the potential threat of information leakage and therefore this information is blocked. There are a lot of n-grams that are first drawn from the statement and later these are looked up for the match from the policy phrase. We have mentioned some of the n-grams that has been drawn from the statement of Mr. A , Mr. B and Mr. X and the ones that are marked in red our those n-grams which were found for match with the policy wall. It can be clearly seen in the figure that only measure of n-grams for Mr. X statement is small compared to the other

two statements and therefore it was allowed to be posted on MCB wall without any threat of information leakage

Case 1: Entropy of sensitive information i-e privacy policy in case of SecureWall, across the wall within same COI. In Facebook and Google+ there is no concept of privacy policy definition for a group. Three types of groups providing three different security levels based on the available privacy options in Facebook, Google + and in Secure Wall. We take these three levels of security as a measure of security for our evaluation, In Facebook were created i-e secret group (Level 1), close group(Level 2) and public group(Level 3). In case of Google+ three groups were created i-e private groups (Level 1), moderated groups (Level 2) and public group (Level 3). Entropy result was calculated based on the mean of the measure for available scenarios. Scale is taken logarithmic due to the fact that difference in entropy was huge because of the absence of privacy policies in Facebook and Google+.

Case 2: Entropy of sensitive information of a group, Figure 15, leaked to the public through group that is through group wall itself to non-members of the group or in case of high level of security that is level1 security, to those members of the groups that are not allowed to see particular information. In SecureWall, every group has the un-sanitized information check. Since the privacy phrase is matched based on n-gram count, therefore, though meager yet there is a chance of information flow across the wall. In case of Facebook, information leakage through group was tested against all the available options and mean value of the three is taken to be the final. Similarly in case of Google + it was checked against the three options. As we can see the results, information leaked in public groups that is with level 3 security is very high therefore entropy of leaked information is also high whereas the security increases the entropy of leaked information decreases. In this case information leakage through group is very meager in case of secret group of Facebook or private group of Google+ for obvious reason as their existence is known to no one except for members themselves. In SecureWall our highest security is unsanitized wall, information can be leaked through unsanitized wall to sanitized wall unless it contains the policy phrases match, and although this leakage does not affect our security concerns yet its measure is shown in the results.

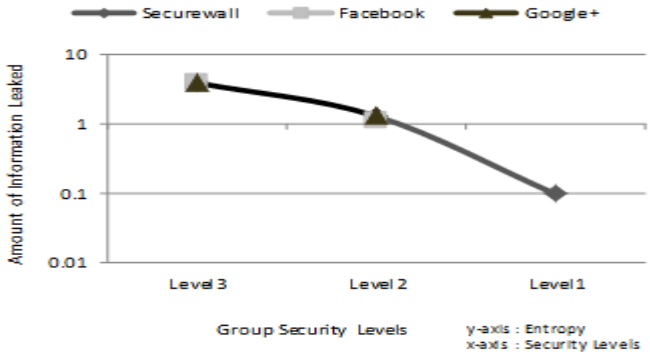

Figure 15. Sensitive Information Leaked Through Group

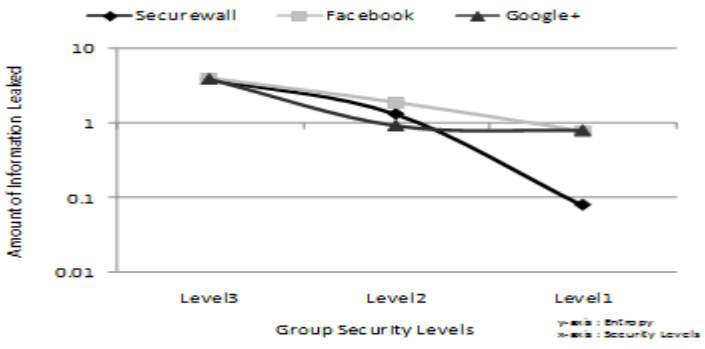

Figure 16. Sensitive Information Leaked Through Members

Case3: Entropy of sensitive information of a group, leaked to the public through members shown in Figure 16. In SecureWall, un-sanitized check is applied for the member user wall. Therefore, the information leakage chance is more or less same as in case of leakage through group wall. In Facebook and Google +, there is no check for the fact that members may post the information outside the group therefore entropy of the leaked information remains high. In Figure 16, we can see that SecureWall information leakage stands at the lowest entropy as members are also checked for information leakage regarding group privacy in case of SecureWall, as compared to Facebook and Google+.

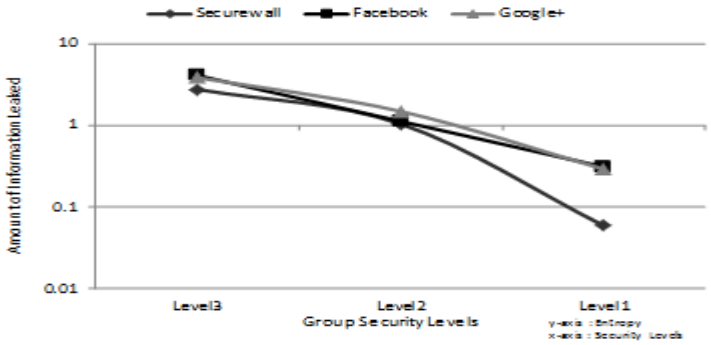

Figure 17. Sensitive Information Leaked Across COI

Case 4: Entropy of sensitive information of a group, leaked to the groups outside the COI, shown in Figure 17. Both group and user can be the reason as group wall has different set of sources of leakage i.e. group members whereas user wall has different source of leakage i.e. friends of any one of group members or member of any other group. In case of SecureWall, chances remain same in both cases. In case of Facebook, chances of leakage through group and user, outside the COI gives high entropy due to high probability of leakage. In case of Google it differs according to the roles therefore, we tested it against available three roles, group owner, manager and member in case of moderated group. Since owner can put access restrictions on manager and manager can put access restrictions on members therefore amount of information exposed to these three roles is different and therefore has different capacity of information leakage. We took average of entropy of information leaked by all the three roles individually and it turned out not very different in results as of Facebook since information leakage capacity through members is still very high in both the cases.

Case 5: Entropy count for individual roles was then combined and mean of the three is taken to be the final case Entropy of information blocked from leakage. This option is not available in either of the networks except for SecureWall. Therefore, we are not comparing SecureWall in this case. We find out the measure of the amount of information blocked wherever privacy alarms are active throughout the site, whether true or false, shown in Figure 18. By privacy alarm we mean that posts that policy bound group user wanted to post and could not be posted. Such posts are matched with the policy phrases defined by the group creator and posts with potential policy information leakage are blocked. These blocked posts are then, checked manually for the relevance of the context. Those posts which were blocked mistakenly only due n-gram match up to the threshold limit which in our case is 45% but the context of the post does not relate to the security concern defined in the policy phrase , such blocks are called false alarms. This gives us a comparison of the total amount of information stopped from leakage, successfully and the amount of information blocked to cause inconvenience to the user in SecureWall. In the graphs results it can be seen that entropy of information blocked as a result of a true alarm lies higher than the false alarms which proves that information that is blocked due to unintelligent act of n-grams is very small. Graph is taken in decimal unit as difference in the entropy of information blocked, in Figure 18.

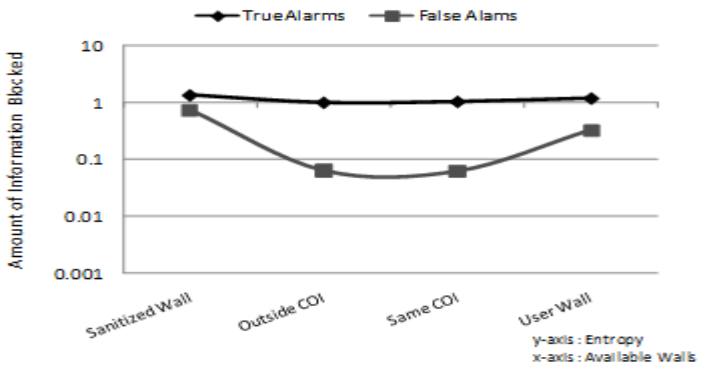

Figure 18. Amount of Information Prevented From Leakage

Case 6: Entropy of information of user A leaked and accessed by friends. User A profile viewed by a friend user B was matched with the information shared by user A to user B. Ideally information of user A shown to user B should only be the one that is shared by user A herself, yet there may be some cases in which information which should not be shown to user B is visible to user B either by mistake or by policy position of that user B. This is treated as information leakage. Similarly, there is some information like user name, or basic information that is used for profile search by search engines is revealed to other users. All such information adds to the entropy of the information of user A profile visible to user B. Such information was checked for being visible rightfully or mistakenly and where ever the match was found it was saved in .txt file and was given as input to the entropy calculator. Entropy of information shared lies at maximum in the resulting graph, as everything shared by user A to user B will remain visible to user B. In case of formal and informal label security clearance of user B there is a difference in entropy compared to high security label and also with low security label.

In case of formal and informal the information leakage chance increases as there is more chance of similarity of information shared to these two groups, a close friend can also be a colleague and user A might want to share formal information with a close friend of high integrity as well. Yet, the entropy of such information is near three decimal numbers, which means there is very small amount of information leaked in these cases.

Case 7: Entropy of information of user A, accessed by a non-friend who is three or more hops away from user A that is a friend of a friend of a friend is considered to be three hops away. Similarly, a user having no connection to any friend of user A or to any friend of friends of user A is considered as more than five hops away. New users having no friends at all in their friend-list served this purpose the best. By trying to access user A profile. Any information displayed to the new user was given as input to the entropy calculator. All the different possible settings were tried and the average of total information leakage was taken. Calculation method remained the same as for case 6. In Figure 19, we can see entropy of personal information displayed is higher than the rest, as basic personal information is required to be displayed in many ways for the network formation for example an old friend of class 2006 , SEECS, Course BIT may search for his class mates through search engines or through the social site itself. For groups all the sanitized information can be found through the user profile to the group itself. Activities remain hidden in our case therefore it shows the least information displayed entropy. For wall and posts multiple options of sensitivity and integrity are checked and average of information displayed entropy is taken as the central one in practice Albums contain very small amount of information therefore the entropy shown is in 4 decimal figures including the case when user explicitly set the low integrity and open security settings for an album.

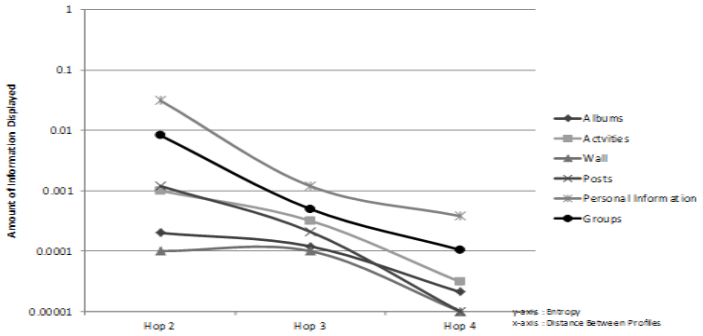

Figure 19: Amount Information Displayed w.r.t. Distance

Case 8: Entropy of information of user A, accessed by a non-friend who is two hops away, as shown in Figure 20, that is, he is a friend of a friend of user A to make a user two hop away we added the new user to the friend-list of a friend of user A. Posts from user A was shared by the friend of user A. Amount of information in the posts or the profile visible to the new user gave the input for the entropy calculation. As mentioned earlier, by information here we mean the text available in comments, personal information exposed through profile, friend's information and posts by the user or his friends. As for pictures or albums, number of pictures is considered as amount of information in this research.

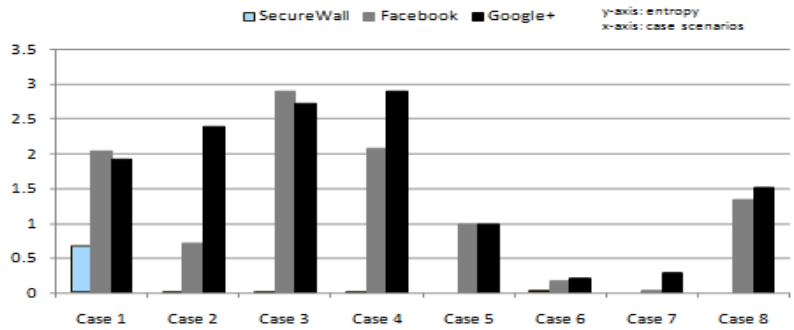

Figure 20. Entropy Measure for All the Test Cases

Figure 20, shows the main results calculated using entropy

In case 7 and 8, since it is a rule of thumb in SecureWall that unless someone's friend request is accepted, he cannot access or read any information therefore the entropy measure of information displayed is very low. In case of Facebook and Google+ users are provided with options if they want their information to be displayed and that too, on individual levels for instance, user needs to specify if he wants his wall to be displayed to non-friend users or not, if they want their friend-list to be visible or not, if they want their display picture or profile information to be displayed or not. This is why the entropy differs in Facebook and Google+ according to different settings by different users whereas in SecureWall it is fixed due to the same level of access to the public for all users. For cases 1 2 and 3, it clearly shows the lack of privacy available at group level at any of the two networks.

7. FUTURE WORK AND CONCLUSION

In this research, we proposed a new aspect for ensuring privacy in social networking sites. Proposed model has been tested by complete implementation of social network and user oriented data has been collected, user's feedback has been utilized to evaluate the system and resulting graphs contain sufficient data to reasonably infer the privacy difference made between the existing approach and the proposed approach. Results obtained from our implementation are satisfactory enough to continue further work in this direction. Aside from the successful results, this system also has some limitations. This system needed extensive coding that was required to first set up a social networking environment in order to implement security rule. This drawback can be avoided to some extent if the idea is to be implemented on an existing and popular social network site but the lattice formation and matrix calculation for assigning access cannot

be avoided. Also, the fine division between usability and privacy limits the proposed system from providing foolproof security.

The fact that the implemented social networking site can have a combination of existing and proposed approach, leads us to a lot of future work options which can ensure the security of the users without making the user themselves to worry about their privacy, keeping the sociability aspect intact. Mandatory Access Control systems in combination of Discretionary Access Control system can also be worked at to result into a hybrid security model. Similarly, the same approach used in our research can be deployed on existing social networking sites to find out the level of security and its effectiveness. For future work this system can be made more intelligent in searching for policy phrases, as we used n-grams for the match, it can be furthered studied how text based classification should be used for more intelligent search and match. There are many other security policies available that has been tried on operating systems and transaction systems etc. but have never been considered to be deployed for social networking purpose. Such other security models can also be used to enhance the security in our implementation. In nutshell, this research has opened a new horizon for research in information security and also in social networking.

REFERENCES

[1] D. Boyd, and E.Hargittai, (2010) "Facebook Privacy Settings: Who Cares?" First Monday, vol. 15, No. 8.

[2] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, (2009) "Persona: An Online Social Network with User-Defined Privacy", SIGCOMM'09, ACM, Barcelona, Spain.

[3] Facebook,"Statistics", www.facebook.com/press/info.php?statistics, Retrieved June 23, 2011

[4] M.M. Lucas, and N. Borisov, (2008) "flyByNight: Mitigating the Privacy Risks of Social Networking", WPES'08, ACM, Virginia, USA.

[5] S. Guha, K. Tang, and P. Francis, (2008) "NOYB: Privacy in Online Social Networks", WOSN'08, ACM, Washington, USA.

[6] S. Jahid, P. Mittal, and N. Borisov, (2011) "EASiER: Encryption-based Access Control in Social Networks with Efficient Revocation", ASIACCS'11, ACM, Hong Kong, China.

[7] H.R. Lipford, A. Besmer and J. Watson, (2008) "Understanding privacy settings in Facebook with an audience view", Proceedings of Usability, Psychology and Security, San Francisco (CA).

[8] A. Felt and D. Evans, (2008) "Privacy protection for social networking platforms" Proceedings of Web 2.0 Security and Privacy, Oakland (CA).

[9] T. Bjorklund, M. Götz, and J. Gehrke,(2010) "Search in social networks with access control",Proceedings of the 2nd International Workshop on Keyword Search on Structured Data, ACM New York

[10] K. Frikken, and P. Golle, (2006) "Private social network analysis: how to assemble pieces of a graph privately", WPES '06, ACM, New York, USA.

[11] T. Wiang, M. Srivatsa, D. Agrawal, (2010) "Network-centric Access Control: Models and Techniques" Technical Report.

[12] D. E. Bell and L. J. LaPadula.(1976) "Secure computer system: unified exposition and multics interpretation" MITRE Corporation.

[13] J. McLean, (1985) "A Comment on the Basic Security Theorem of Bell and Lapadula" Information Processing Letters, vol 2, No. 20, p 67-70.

[14] Gross, Ralph, A. Acquisti, and H. John Heinz III, (2005) "Information Revelation and Privacy in Online Social Networks" WPES' 05, ACM

[15] M. Sahlabadi, H. M. Deylami, (2009) "Refactoring for Security in Social Networking Applications", Kaspersky Lab International Cybercrime Conference.

[16] M.Bishop, (2003) "Computer Security: Art and Science", Addison Wesley, Boston, MA.

[17] K. J. Biba, (1977) "Integrity Considerations for Secure Computer Systems", The Mitre Corporation, Technical Report, N°MTR-3153, Rev. 1.

[18] IETF, "RFC 1457", "Security Label Framework for the Internet" http://www.ietf.org/rfc/rfc1457.txt, Retrieved September 02,2011

[19] R. S. Sandhu, (1992) "Lattice-Based Enforcement of Chinese Walls", Computers & Security, vol. 11, No. 8, p 753-763.

[20] Oxwall, "Oxwall Software" http://www.oxwall.org/, Retrieved July 18,2011

[21] D. Godes, D Mayzlin, (2004) "Using Online Conversations to Study Word-of-Mouth Communication", Marketing Science, Vol. 23, No. 4.

[22] GO-Gulf, "User Activity Comparison Of Popular Social Networking Sites", http://www.go-gulf.com/blog/social-networking-user, Retrieved May 02, 2012

[23] B. Streisand, "Entropy Text Analyzer", http://miup2002.fc.ul.pt/problemas/I/I.html, Retrieved July 28,2012

[24] N. Razzaq, "SecureWall", http://www.technolx.com/nrmciit/ , Retrieved September 14, 2012

Author

Nadia Razzaq obtained her bachelor's degree in Software Engineering and MS degree in Computer and Communication Security from School of Electrical Engineering and Computer Sciences, National University of Science and Technology, Pakistan in 2013. She is working in Cyber Security Department of Pakistan Military. Her research is centred on privacy in social networks