Security Challenges and Approaches in Online Social Networks: A Survey

Racha Ajami, Noha Ramadan, Nader Mohamed, and Jameela Al-Jaroodi
{rashaaj, noha-ramadan, nader.m}@uaeu.ac.ae, jaljaroodi@gmail.com
Faculty of Information Technology, UAEU
P.O. Box 17551, Al-Ain, UAE

Summary
Social Networks (SN) Sites are becoming very popular and the number of users is increasing rapidly. However, with that increase there is also an increase in the security threats which affect the users' privacy, identity and confidentiality. Different research groups highlighted the security threats in SN and attempted to offer some solutions to these issues. In this paper we survey several examples of this research and highlight the approaches. All the models we surveyed were focusing on protecting users' information yet they failed to cover other important issues. For example, none of the mechanisms provided the users with control over what others can reveal about them; and encryption of images is still not achieved properly. Generally having higher security measures will affect the system's performance in terms of speed and response time. However, this trade-off was not discussed or addressed in any of the models we surveyed.

Key words:
Security, social networks, privacy, anonymity, peer-to-peer, mobile social networks.

1. Introduction

SN sites are defined as interactive web-based applications that provide users with the ability to communicate with friends and family, meet new people, join groups, chat, share photos, and organize events and network with others in a similar-to-real-life manner. SN functionalities are organized into three main categories: Social Networks Services (SNS), Network Application Services (NAS), and the communication Interface (CI). SNS are used to establish social network relationships between people who have the same activities and interests. NAS provide network interaction services for users such as psychological tests, social web games, fans groups, etc. CI offers platforms to support users' communication and interaction. The *privacy paradox* is an interesting phenomenon that takes place in SN websites, where people are usually more protective of their personal information when using different communication media (i.e. Personal or Phone) compared to their readiness to provide this information via the SN websites.

The Internet connects the whole world over this digital network which makes it more difficult to protect information using traditional technical solutions. Knowing the purpose behind information theft and attacks on SN sites helps in providing the best techniques to protect the users' information [16]. Attackers and fraudsters might attack just for fun, and to show that they can penetrate secure systems, others might attack to gain control over systems to organize devices into a Botnet to apply DoS attacks. However, the most common reason is the financial benefit gained by collecting user's critical personal information such as bank accounts, social security numbers, and passwords. By doing so, attackers can commit identity theft crimes and generate profit. There are different precautions that should be considered beside the technical solutions. These include raising users' awareness to help them distinguish between sensitive and public information. In addition, SN sites should play a major role in protecting personal information. They should enhance spam and malicious links filtering, notify users when any attack takes place, and program the sites carefully to be protected against platform attacks and other attacks likes the SQL injection and Cross-Site Scripting (XSS) which can be added to the web page code to steal cookies, force users to download malware and hijack users' accounts [17].

This paper will highlight some issues related to the security of SN sites. In Section 2: we introduce the users' requirements and perspectives when it comes to their privacy and confidentiality. Section 3: includes the main challenges facing privacy measures. In Section 4 we offer a discussion of different approaches of SN security. Section 5 includes a comparison of the discussed approaches and Section 6 highlights some open issues and security needs that were not covered by the approaches we studied. In Section 7 we conclude the paper and summarize our observations.

2. SN Security Requirements

As people are unaware of the dangers of the socio-technical attacks, they usually uncover everything about themselves via the Internet thinking that this information does not affect their privacy. The willingness to uncover personal information on SN websites negatively affects

Manuscript received August 5, 2011
Manuscript revised August 20, 2011

their professional and even their personal lives. The security firm Sophos [18], Nagy and Pecho [15], conducted a study on social network users to test their awareness of protecting personal information. Both studies showed profiles of midrange college educated users living in a modern city. Sophos conducted the study in the European region while Nagy and Pecho tested users in USA. When comparing the results of both studies, it was found that the understanding of what is considered as critical information varies between Americans and Europeans. Generally information about residence and career got lower response from Americans. However, Europeans were more protective of personal information such as Phone numbers, E-mails, IM contacts and Education. In general, there are some basic requirements for security in SN sites including the following:

- Registration and login: The registration phase is needed to grant network access to the user for later authentication. After registering users acquire a unique User ID and authentication information which should be stored confidentially and with integrity.
- Access Control: Distinguishing between users and groups access privileges is very important to determine the users and groups ability to access the private and/or shared items or the different profiles. Access control is also needed to manage groups with thousands of users. So access control aims to ensure the integrity, confidentiality and availability of shared items.
- Secure Communication: During instant messaging and live chats, messages must be directly sent to the addressed receiver, so senders and receivers must be authenticated, and the communication itself should provide confidentiality and integrity.

3. SN Security Technical Challenges

SN sites are perfect for illegal online activities as they consist of a huge number of users with high levels of trust among them. As a result there is a high range of security risks, threats and challenges. Here are some of these security challenges and some proposed solutions from the surveyed projects which will be discussed in section 4.

- **Privacy risks**: SN sites provide some mechanisms for privacy settings to protect users, but these mechanisms are not enough to protect the users. The top and primary privacy problem is that SN sites are not informing users of the dangers of spreading their personal information. Thus users are not aware of the extent of the risks involved. The second problem is the privacy tools in SN sites, which are not easy to use and do not offer the flexibility for users to customize their privacy policies according to their needs. The third problem is the users themselves who can not control what other users can reveal about them such as tagging their photos or related information to other friends' profiles.
- **Security risks:** Social Engineering uses fake SN accounts to notify members to reset their accounts or they send malicious e-mails as security notifications. Revealing personal data is another security risk as SN sites may contain many applications developed just for hacker disturbance and revealing user's personal data. Drive-by Download is also considered a security risk. Some SN applications may include malicious links or codes, such as requesting users to download a specific program to run these applications. Phishing is another security risk. Some applications such as psychological tests and different type of personality tests use fake web pages just to collect users' data through some seemingly harmless questions. For example, in some applications the user is requested to enter the cellular phone number to receive the test result, using this number, the attacker can embezzle some money from the phone's credit. Sometimes phishing attackers send a message to a user's SN imposing as a friend asking the user to visit a malicious and fake SN login page. If the user goes to the page, the attacker can steal the user's login credentials to initiate future attacks. In addition, Trojans are considered a security risk as they use fake SN accounts to send e-mails to users to update their passwords. These usually ask the users to open an attached file to update their password. Once that is done, a Trojan or other malicious programs will be downloaded. A fake Friendship invitation is a security risk also which uses the concept of the identity theft by using false friend's data to add other friends and to steal their data. Criminal Cases can be considered as a security risk as terrorists are using SN sites to achieve their targets.
- **Anonymity risks**: These attacks target the users' identity and privacy. A direct anonymity attack tries to compromise the users' anonymity by exposing their information and location while connecting to a SN site via mobile devices. As mentioned, devices that are in the same system can find the name of the SN user which will directly compromise the user's privacy. An indirect or K-Anonymity attack takes place when several pieces of information that are independently non-compromising indirectly compromise the users' identity by putting these related pieces of information together to map back to users' identity. For example, list of favourite stores and restaurants of a certain user can easily be used to track a user and find his/her location.
- **Other risks:** There are many other sources of risks on SN that may compromise the user and or the SN providers. Some of these may be physical risks while most are logical. Some examples include:
  - Connecting home devices to a SN site may expose more information about the users within the

household. This may cause unprotected devices to compromise the others within the home network.

- Protecting from SN site operators is essential since exposure to the operators and maybe their partners may cause risks on the SN and its users. The possibility of large-scale privacy breaches on the SN sites can compromise some or all users' data available on the SN site. An intentional or even unintentional data disclosure will cause a large-scale privacy breach.
- Users dependence on the service provider's existence may also be risky since many of the SN sites are run as free services and those providers may disappear any time which basically leaves users with no access to any of the information they keep on the sites. Spoofing the system using false identities or colluding in small groups may provide access to others' personal information.
- Trust among users and with service providers is hard to achieve and the lack of it pauses great threats on the success of SN sites. Users need to establish strong trust relationships with each other and with the service providers and in many cases with the service providers' partners. This is a challenge since it is hard to provide concrete methods to create trust or maintain it.

4. SN Security Approaches

SN sites have become more popular recently and their users are increasing rapidly, but there are many security threats that can affect the users' privacy and confidentiality. The SN sites functionalities include three main categories: Social Networking Services (SNS), Network Application Services (NAS), and the communicate Interface (CI). Some SN security approaches have already been proposed. In this section, different approaches will be presented in details and evaluated to explore their advantages.

4.1 Proxy-Based Real Time Protection

The proxy–based real time website security protection mechanism [1] uses the concept of Cloud Computing and its main function is detecting the websites security threats. The concept is to combine several online security scanning services and protection software to scan a webpage's security. Once security threats are found in a webpage, they will be blacklisted by the system and a warning will be issued to the client whenever a blacklisted webpage is accessed. This approach can decrease the security risks in SN and prevent using risky or blacklisted websites. In addition, it provides warnings every time the clients try to access a risky or blacklisted webpage. This approach improves and develops the scanning correction rate, and it prevents users from accessing security compromising websites. However, there are some disadvantages for this mechanism. One of which is that it needs to be updated periodically and network connections need continuous maintenance.

4.2 P2P Based Social Networks

Social Networking Sites are web-based platforms consisting of millions of users and participants in social networks sites, and the P2P approach solves the load and the cost issues but leads to new security issues and challenges. SN supports security requirements in different aspects such as the registration, authentication, access control, and confidentiality.

Security framework for P2P-based platforms for SN [2] supports the users' registration and login process, where a new user chooses a unique username and password to generate an asymmetric key pair PrivA, PubA. In the login process the user recreates the key pair after entering a valid username and password. The user ID is used to encrypt the communication to this node/user, only the receiver can decrypt these messages. In addition, it supports access control as different users have different access rights such as reading shared items, creating new shared items, and altering existing files. A shared item that needs access control is encrypted with an object–specific key. Moreover, in the case of instant messaging and chats, each message is signed by the sender and verified by the receiver. For example, user A sends an encrypted message containing the symmetric key encrypted with the public key of user B (the receiver) and signed with the sender's private key. The receiver (B) verifies that the message is from user A using A's public key. If user B accepts the communication, the symmetric secret key is used for consequent communications. Most of the security requirements are nearly solved using the P2P-based platform. It provides direct connections to share information easier and faster than uploading through e-mails.

4.3 U-Control

The privacy issue in SN sites is very important. As a result, a new framework is being presented to enable users to control the sharing of their sensitive personal information and control their privacy on SN. The proposed framework called U-Control [3] supports and facilitates digital persona and privacy management (DPPM). The U-Control framework enables the main services such as **(1)** Identifying Attribute Management by giving a privacy numerical rating from 1 (least sensitive) to 5 (most sensitive) for each user attribute. The rating depends on the following characteristics: data type, data user, data

usage, and data validity. It also depends on personality, financial, and identifiably factors. **(2)** Selective Attribute Disclosure and Sharing using an ordered skip list to search and update an element (x) using three operations *find(x)*, *insert(x)*, and *delete(x)*. The U-Control system architecture consists of functional component-based system architecture and operational system architecture. The functional component-based system architecture is composed of three systems which are U-Control attribute provider, a U-Control agent and a social network.

Performance evaluation was done for this prototype in terms of the attribute proof size and the credential generation time. The results show that the average proof time is easily predictable. Verification time is very important as SN sites process immediate verifications for many different users at the same time and must provide results in real-time. As a result of this analysis and evaluation, the approximated complexity is O (v log (n)), where v is the number of attributes to be disclosed and n is the number of attributes contained in the record.

4.4 Privacy Protection issues in SN Sites

Nowadays, SN sites are attracting a huge number of users, however; there are many security risks and threats associated with them. The main purpose of SN sites is sharing information and keeping in contact with users of different relationship levels such as Best Friends, Normal Friends, Casual Friends, and visitors. For each profile in a SN different types of Users' Data are included such as identity, demographics, activities, and added content. Different users have different privacy concerns for their different kinds of information; therefore, four privacy settings are being proposed for the users' data according to its impact on different users' privacy preferences/settings [4]. These are: healthy data (general information about users), harmless data (demographic information), harmful data (inappropriate posts that affect the user's reputation negatively), and poisonous data (very secure data for the users). As a result, four levels of privacy have been adapted on SN sites: no privacy, soft privacy, hard privacy, and full privacy. Moreover different tracking levels are being adapted which are strong tracking, weak tracking, and no tracking. The proposed privacy framework may cover different privacy cases, but normal users need to spend more time to understand and configure their privacy Settings. A study points five prototypes of SN users which are Alpha Socialisers, Attention Seekers, Followers, faithful, and functional.

The framework is able to classify users in the appropriate prototype based on their characteristics. An appropriate privacy level can be proposed for the users based on their provided information for SN. If the information provided by the user is not enough, the framework will set the default privacy level which is hard privacy and soft/weak tracking and it can be customized by the user later. This approach helps users to determine their required privacy levels, and have a good amount of information about the future potential risks in different activities. The problem is that these existing solutions could not be enough as the main purpose of SN is to share information and contact people. In addition, there are some privacy problems in SN such as lack of users' awareness, privacy tools are not easy and not flexible, and finally users cannot control what others reveal about them.

4.5 Home-Network Social Application [5]

Information is spreading nowadays through SN sites not only through the information provided by the users, but also through gathering information about the users' habits, preferences and routines using inputs from the user's access/usage behaviors and from connected home devices like set-top boxes and media gateways. Enabling that link between those home devices and SN sites puts users' information at a higher risk if not handled in the right way.

The new architecture creates two main applications, Social Enabler (SE) and Social Watchdog (SW). Those applications can be embedded in the home gateway, in the home device or on the home network. The SE is an intermediary between the SN site and the user to ensure the correct representation of the across the different devices. The request sent from the user contains the username, the requested resource, device constraints and the requested operation. While sharing multimedia components the requests will contain username, live stream, content type and the sharing request. The SE handles the authentication from the SN site while collaborating with the SW to retrieve the requested content. The SW is responsible for the security and privacy issues in the request communication. It provides credentials for the devices as well as parental controls. SW is designed to handle requests as fast as possible by maintaining a set of authenticated requests and devices for a certain time during which all requests sent from the same device within the validation period will be handled faster than those sent by other devices. The Watchdog in the SW generates periodical reports about what was published by the user, the user's home devices and the user's friends. However, those reports can be controlled by the user to restrict the amount of reports collected and what can be accessed.

This approach helps in allowing home devices that are rich in users' information to actively participate on behalf of the user in SN sites. However, the system needs to improve policy management for the home user to give him/her the right to monitor and understand how policies

are applied by the SW while reading the reports in the home gateway.

4.6 Privacy-Enabling SN

To remove the dependence on the social network operator many approaches chose to distribute the system. Privacy-Enabling SN [6] makes it possible to preserve the simplicity and performance of the Client-Server model. The model helps not only in protecting users' information from other users, but also protects users' privacy against the SN operator. Moreover, all previous work recommends encryption to hide users' information, but none approaches the concept of hiding the links among users as a solution as in this model. The model composes the client into four layers, starting from the top there is Application Layer, then the Data Structure Layer, the Cryptographic Layer and finally the Network Layer. In the application layer, applications run inside a secure sandbox that helps in controlling the access to users' data and all related communication channels. The Data Structure layer encapsulates the user content as a collection of discrete blocks includes the links to other authorized blocks. The privacy assurance takes place when hiding those links between the blocks that is forced by the Cryptography layer and provides confidentiality by preventing unauthorized users to access and view users' content. Finally the Network Layer assures the simple interaction between the client and the server.

As mentioned, the model protects users' information not only from unauthorized users, but also from the network operator. To adapt the simplicity of the centralized server, it makes it impossible to prevent that server from analyzing the traffic in the controlled network.

4.7 Identity Server and Anonymous Identifier

Mobile phones are no more used just to make phone calls. They have been promoted to Smart phones that can handle most of the applications carried out by a computer such as office applications, Internet browsing and online SN access. Communicating wirelessly with SN sites or any application over the Internet compromises users' anonymity and make their information a victim to eavesdropping, spoofing and wormhole attacks. Whether the mobile device is a part of a Peer-to-Peer mobile SN system or a client-Server mobile SN system, the identity of the user is not anonymous. In P2P SN systems the user can be tracked by collecting the login dates and times of a user and creating a history of visited locations of the user. The client-server SN system also compromises the users' anonymity by exposing the user's location since each device that is connected to that system will have access to the SN user names of nearby users.

This approach [7] provides certain functions that link a user anonymously to use in third-party applications. By that, the user's identity will be hidden while requesting information and applications from SN sites. This privacy protection can take place when adapting the approach of Identity Server (IS) and its Anonymous Identifier (AID).

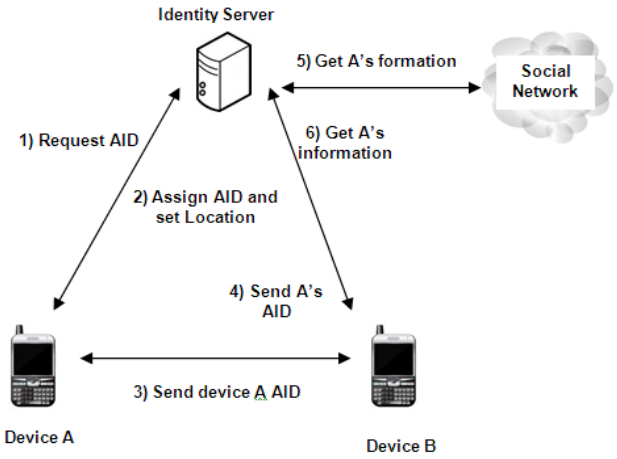

Fig. 1 IS and AID mechanism to link a user anonymously while using a third-party application.

The process starts when the user securely contacts the IS to request an AID as Figure 1 shows, the AID will be generated with a cryptographic hash function and sent to the user's device. When another device establishes a connection with that device (device A) through a Bluetooth or a Wi-Fi connection, the generated AID will be shared between the two devices. To establish another connection with another device, device A will repeat the same process to get a new AID for the new device. When device B gets the AID, it will retrieve the required information from the SN Profile through the IS. After getting user's A preference and information, the IS deletes the AID of device A from the list of the AIDs associated to device A, then sends the request back to device B. To ensure efficiency, multiple AIDs are associated to one device to allow it to establish many connections and the same time, but to prevent the growth of AIDs list per device; a timeout period is set. When an AID time is out, IS will remove it from the device's associated list. In addition to protecting the anonymity of the user's location, this application prevents eavesdropping by encrypting all network traffic that flows between the devices to the IS. However, the implementation of this approach was tested in the limitation of the range between the devices that are being authenticated and sharing the AIDs to retrieve requests from social network sites.

4.8 Virtual Individual Servers (VISs)

Would it not feel better when you own and have total control over to the content you upload to SN sites or any other third-party service? Virtual Individual Servers (VISs) [8] is a virtual machine that runs on a computer infrastructure with high availability utilities. One of the most important advantages of VIS is providing long-term availability. In centralized third-party services the user depends on the availability and existence of the provider. In contrast, VIS users can make a complete VIS image backup elsewhere and resume whenever is convenient. In addition, VIS helps in improving users' privacy by giving the users control over their private data and what information they allow to be shared. Moreover, VIS provides flexibility to the owner to install software packages and set their own preferable configuration options and functionality. Running and controlling wide range of users' data in one centralized third-party server set the users as victims to large-scale privacy breaches. VIS is resistant to such breaches because each user owns his administrative domain. Also, VIS has an advantage over the mobile device that directly shares data, in which VIS is not limited to energy constraints of those.

One of the applications of VIS is the participatory sensing. Mobile devices nowadays are embedded with different sensors such as GPSs and Cameras that help in collecting a wide range of data that can be used in many applications. However, the user in there has little control on what information is collected from the device as well as what is affecting the device's performance and battery life due to the number of applications that will be running on it. In the VIS scheme, the user uploads collected raw data only once to its VIS which has all the required applications and interacts on behalf of the user with the sensing server according to the predefined user's specifications and limitations. Problems with VIS are very limited compared to the benefits provided. One problem is that users need to manage their own virtual machine and take full responsibility of that. Cost is a problem as well, since the user will need to pay for the computing and storage resources needed by their VIS.

4.9 FaceCloak

FaceCloak [9] is an architecture that helps in protecting users' information from other users as well as the service provider. The user has the choice to provide protection for certain information and leave other parts unprotected. Many other approaches assumed that the SN site is trusted; however that should not be the case. This approach mainly functions automatically and requires no or little configuration by the users. It also requires no modification of the SN architecture, which is mostly unacceptable by the service providers even when their users' privacy is at risk. Moreover, FaceCloak is a self-contained architecture which requires no additional software to be installed by the user and minimal configuration on its side. In addition, the architecture assures communication between the users that implement it and those that do not. Both existing SN users and new ones can benefit from that approach. Existing users can protect any new posts or messages sent and new users can force privacy protection on all the information posted in their profile such as their names, ages, birth date and gender.

The architecture includes three phases, Setup, encryption and decryption as shown in Figure 2. The Setup phase starts when the user installs FaceCloak to the browser, then, three keys will be generated, master key, personal index key and access key. A copy of the first two keys will be distributed to the user's friends using a tool provided by FaceCloak, whereas the access key is locally stored. Users profile, messages and blogs are stored in an encrypted form in a third-party server that will be set up in this phase.

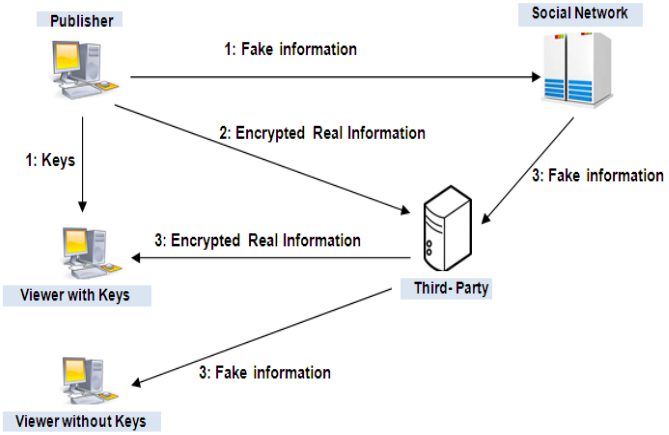

Fig. 2 Basic phases of FaceCloak Architecture

The Encryption phase takes place when posting or entering any text to the site with a special marker that is predefined as "@@", and if the user wants to reveal any part of the profile, the text can be added normally. All the text that has that special marker will be replaced with a fake text that is not randomly created and has some meaningful context such that the operation is unnoticeable. In the decryption phase, the page that was requested by a user without the master and personal index key will be received with the fake information, on the other hand, if the user is authorized, the information will be matched with the index of FaceCloak and send the real information to the user.

The problem of users' awareness of what information is sensitive and should be protected still exists with this approach. In addition, if the SN site colludes with the third-party server it can easily detect a FaceCloak user and suspend the user from the site. The most dangerous

problem, however, is that if an attacker takes control over the user's browser; he/she can disable/uninstall the extension of the architecture and even get the access key to the third-party and access the user's private information.

4.10 FlyByNight

Many approaches exist to protect users of SN sites from the service providers and FlyByNight [10] is one of them. It is a facebook application that is downloaded to the users' browsers for encrypting sensitive data using a client-side JavaScript. The architecture phase starts when the user first interacts with it after the installation. It generates a public/private key set and generates a user password, all in the client-side JavaScript. When the user adds posts or updates a piece of information on a profile, he/she enters it in the application that has complete access to the list of the user's friends who already have installed the application. The Java-Script then encrypts the data with the "public key" and tags it with the ID numbers of the recipients. The encrypted data is sent through Facebook to be saved in the application's message database. That way, the message existence will be public, but the content is encrypted. When the user requests the new messages or any updates from the application's message database; a cipher text version is delivered. The user uses the set password to decrypt the "private key" that in turn is used to decrypt the message.

This architecture protects Facebook users' privacy in many ways; it ensures that the Facebook server never stores clear text data of the user and protects users' data from being misused by Facebook employees. Moreover; this application ensures the ease of use by simply downloading it to the browser and it also provides one-to-one and one-to-many communication. However, the design did not achieve the level of encrypting images, which is one of the most commonly posted items on Facebook and affects users' privacy.

4.11 Reputation Mechanism using SN Sites

The Reputation Mechanism [11] is a part of a recommendation system used as both a main component in peer-to-peer transactions and in online SN by allowing users to personalize recommendations via users they trust. Using these networks leads to network integrity and minimizes users' privacy concerns. Using SN with a reputation mechanism can be useful in two ways: it offers an automated aid to identify reputation and rating based on position in the network structure; and it works as a filtering tool for users' ratings.

There are several benefits and challenges of using reputation mechanisms with SN. It makes it more difficult to spoof the system through creating false identities. False identities will limit their connection with only their old friends or disconnect themselves from SN as a whole. On the other hand, the false identities can still keep the connection relationship with their friends, who are still connected with others, to have access to their information. If the reputations are being filtered by excluding the explicit rating from friends and friends of friends of the person being evaluated, altering reputation scores will require collusion outside of one's identified social circle that is more difficult than the collusion among people who know each other already. However, sometimes participants can sell their identity to others; which leads to a huge security threat especially if this user has a good reputation.

4.12 Reputation for Directory Services (ReDS)

P2P architectures are very important for online SN and mobile SN applications such as Skype. P2P systems are providing directory services which are decentralized to locate peers with their required content, services, and data. To secure directory services in open P2P systems a Reputation for Directory Services (ReDS) [12] framework for using reputation management to improve and enhance the security of locating information in distributed systems, has been proposed. Salsa is a structured P2P directory service with redundancy based on a virtual balanced binary tree and nodes are organized into several groups. Nodes know all their peers and neighbors under the same group (local contacts) and some of the nodes that are from other groups (global contacts). Salsa uses redundant lookups as a node requests the subset of its local contact to look for the same target. Global contacts are located and selected randomly. This randomness provides path diversity and prevents the redundancy of lookups through using the same node in the lookup. There are several benefits for Salsa. For example if a requesting node received conflicting results, the actual target owner will be the closest to the target by definition. On the other hand; there are some limitations as it uses redundancy and path diversity to reduce the lookup failures. There remains a number of failed lookups for reasonable redundancy levels. However, a small fraction of the total number of lookups failures can hurt the system's integrity. The most important target is to reduce the amount of redundancy and to reduce the failure rates.

Reputation for Directory Services has been applied to Salsa to be Salsa-ReDS which takes advantage of the redundant lookups and the ability of the requesting node to

identify the correct result. The local contacts which provide correct results gain positive reputation, and those nodes which provide incorrect results gain negative reputation, so it will be easy to identify the reliable local contacts and the malicious nodes.

4.13 Semantic Web Based Framework

Online SN include lots of personal information which leads to opportunities and challenges. This information can help a lot in marketing activities by targeting specific types of users; however, privacy and security concerns can prevent such activities. Different SN implemented different types of access control, Facebook supports the option "Selected Friends" & "Friends of Friends". These options have the advantage of being easy but they are not flexible as they are too restrictive in some cases and too loose in others. Because of these limitations a semantic web based framework for social network access control has been proposed [3]. The resource description framework (RDF) and the Web ontology language (OWL) have been used for modeling SN data. It models the following five important aspects of SN sites: Modeling Personal Information, Modeling Personal Relationships, Modeling resources, Modeling User/Resource Relationships and Modeling actions

In Facebook, *Modeling Personal Information* uses "friend of a friend" Ontology (FOAF) which is an OWL based format used for presenting an individual's SN information. It provides different classes with properties to describe SN data, so FOAF can be used to capture personal information available on SN sites. *Modeling Personal Relationship* is done using an n-ary relation pattern. A FriendshipRelation class is defined with several subclasses such as CloseFriend and DistantFriend that denote the strength of friendship. Each one of these has been created without creating detailed subclasses. *Modeling resources id done* through creating Resource classes with several subclasses with unique properties and relationships. For example Messages have a sender, a receiver, a subject, a message, and a timestamp. There is also a subclass for messages called WallMessages, which is similar to the message in its data properties but it has more restrictions as it can be sent only to a single individual wall. *Modeling User/Resource Relationships* assume that the only relationship between resources and users is the ownership. However, from the access control's point of view this is not enough. In case of a photo album, for example, two classes have been created: the Photo class and the PhotoAlbum class which are linked through the containsPhoto relationship. The person who uploads the photos is indicated by the ownsAlbum relationship. *Modeling actions which* actions are defined as object property that relates users, resources, and actions is done through hierarchical models created for the actions.

Several Security Policies for SN sites are supported by Semantic Web based frameworks have been outlined. Examples are access control policy, filtering policy, and admin policies that depend on trust relationship among various users. However, implementing this prototype using a java-based open-source semantic web application development framework called JENA is more beneficial as it offers an easier programmatic environment to implement these ideas.

4.14 Re- Socializing Online Social Networks [14]

There are several requirements for SN users those need to be carefully analyzed. These include information self determination which requires that users' profiles and personal content may not be disclosed to any other users than the trusted contacts. As a result, all communication must ensure security against man in the middle attacks. A manageable secure mechanism is also required to publish a selected profile attributes depending on the trusted contacts, control profile personal data, and the ability to terminate the user's own online SN account. Strong trust relationship is another requirement which limits the maximum length of the chain of trust to one-hop relationships. However, the user should be able to contact with two-hop relationships, but user should not be able to publish profile information of his one-hop relationship. Profile availability is also a requirement since online SN sites are worth nothing if the published profile information is not accessible at all. Thus securing online publication is needed to allow safe access to data while its owner is offline. Mobility Support is an additional requirement as users need special support for mobile devices which currently suffer from limited bandwidth, computing power, and have problems with complex user interfaces.

As a result of all these requirements, a novel decentralized multi-domain SN was designed. Multi-domain SN is based on categorizing the SN into the following three domains: social Webspace, social Mobilespace, and social Homespace.

To connect with other users there are two proposed basic schemas which are out-of-band invitation (OOB) and coupling. In *OOB*, users A and B, for example, agree on a PIN code or password then user A sends an e-mail to user B containing the link to the SN, the exchanger address, the link to the public key and some explanatory text. User B can send a message to user A which contains a new link to the public key, the exchanger address, and secure message authentication code. After that, user A will refresh the key, then a secure channel will be established so both users will be ready for secure communication. *Coupling* is another mechanism that supports implementing new one-hop relationships between users B and C where user A has introduced his two friends to each other. This maintains a

two-hop relationship through user A. User A sends a coupling request to users B and C which contain parts of B and C profiles which are marked as public. User A will receive both responses and then the encrypted messages will be forwarded to users B and C. Users B and C will perform a key refresh to comply with the strong trust relationship. As user A knows about the link public key which was applied during the coupling, it depends on the trust level between A and B and B and C, then the key refresh can be trusted without another OOB process. The coupling mechanism supports the idea of organizing groups by a virtual network user who is taking the role of user A.

5. Comparison and Discussions

We surveyed different existing SN Security mechanisms and approaches. In addition, these approaches will be evaluated with respect to the challenges and constraints such as: flexibility, operator protection, user anonymity, and dependency on the provider's existence.

Virtual individual servers (VIS) [8] are virtual machines that run on a computer infrastructure with high availability utilities; VIS is used to upload contents to SN sites or any other third-party service. VIS provides independence from the Service provider because it provides users with the ability to get a complete image of the information with the service provider, which allows them to resume usage whenever needed regardless of the providers' existence. Moreover, in VIS users' are free to add or remove functions at their convenience but they need to manage their own machines and afford the cost for the computing resources used by their VIS. Users' Anonymity and Protection from the service provider are not fully achieved in the default situation, however, the user can install arbitrary operating packages and set their own configuration options to achieve their target of anonymity and even security.

FaceCloak [9] is a self-contained architecture that provides a full flexibility to users. It functions automatically and requires no or little configuration by the users, and requires no modification of the social network architecture. Add to that, it assures communication between the users that implement it and those who do not. Moreover, FaceCloak helps in protecting users' information from other users as well as the service provider by encrypting the information and making it appears as fake data that could not be decrypted without having the required keys. But, this architecture does not help in providing independence from the SN provider's existence.

FlyByNight [10] encrypts sensitive data using a client-side JavaScript. Its flexibility resides in the ease of use from the users' side. All that need to be done is download the application to the browser and identify the list of friends that will be receiving the encryption keys. By doing so, the users' information is protected from the Facebook system administrators and employees and from other users who do not have the required encryption keys. Once more, the users' data existence depends on the service provider's availability.

The proxy based real time protection approach [1] uses the concept of cloud computing to provide a secured networking environment for the Internet users. It is a flexible mechanism as no much involvement is required from the users. The user just uses the browser for visiting a webpage, the browser redirects the request to the proxy. The proxy will scan the site and decide whether to allow the connection or to blacklist the URL and send a warning message to the user. Any user requesting a blacklisted site will receive a warning message. This protection is provided by the operator itself. Moreover; this mechanism does not provide a backup for the users' information available on the SN service provider, so users' profile and information existence depends on the availability of the provider.

The P2P-based SN approach [2] supports the security requirements which are registration and login, access control and secure communication. This mechanism depends on the provider's yet it is flexible as it allows authentication of the users easily. Users and applications communications are confidential and are authenticated. Access control solutions are also provided for both individual users and group of users. Moreover; each message sent between the users is signed by the sender and verified by the receiver.

The U-Control mechanism [3] enables users to control the sharing of their sensitive personal information and control their privacy levels in SN sites. It supports and facilitates digital persona and privacy management (DPPM). It is flexible for experts to control and manage their privacy while it is not for normal users. This mechanism depends on the SN provider's existence for the users. The protection is supported by the operator itself as users' information and messages are encrypted against other users on the SN.

The privacy protection issues in SN sites approach [4] classifies users in the appropriate prototype based on their characteristics and purposes the privacy for the users according to their provided information for SN. This approach helps users determine their required privacy levels which make it flexible in some ways yet it is not easy and flexible enough for normal users. For example, if the information provided by the user is not enough, this approach will set the default privacy level then the user can customize it later. The protection is supported by the operator itself as users' information and messages are encrypted against other users. This mechanism depends on the provider's existence as well.

The reputation mechanism [11] is the main component in peer-to-peer transactions and a part of the recommendation systems. It is a kind of an easy mechanism as it depends on the peer-to-peer mechanism which allows users to personalize recommendations via their trusted friends or users according to their reputation. However, it is difficult sometime to recognize the reliable or trusted users despite their good reputation and the high rating. This mechanism depends on the provider's existence and provides an operator protection as users' information, messages, and communication are encrypted and authenticated.

ReDS [12] is a framework for using reputation management to improve and enhance the security of locating information in P2P distributed systems. ReDs is somehow flexible for experts, but not for normal users. However, it does not require much involvement from the users. It provides an operator protection as users' information, messages, and communication are encrypted and authenticated between the communicating nodes. Therefore, it is easy to identify the reliable local contacts and the malicious nodes. The existence of users depends on the existence of the provider, as this mechanism does

Table 1: Approaches for SN Security

Project Name	**Main Features**	**Flexibility**	**Operator protection**	**User Anonymity**	**Independent from provider existence**
Home-Network Social Application	Enables SN interaction in home devices while preserving users' privacy and control.	Some	No	N/A	No
Privacy-Enabling social network	Protects private information against discovery and disclosure from users and service provider	Yes	Yes	Yes	No
AIDs	Links a mobile user anonymously with the user's location and hides the user's identity while requesting information from SN websites.	Some	Yes	Yes	No
VISs	virtual machine that runs on a computer infrastructure with high availability used to upload contents to SN sites or any other third-party service	Some	Some	Some	Yes
FaceCloak	self-contained architecture which requires no additional software to be installed and helps in protecting users' information from other users as well as the service provider	Yes	Yes	N/A	No
FlyByNight	facebook application that is downloaded to the users' browsers for encrypting sensitive data using a client-side JavaScript	Yes	Yes	N/A	No
Proxy-Based Real Time Protection for SNS	Detecting and determining the websites security threats and blacklisting the none-secure WebPages	Yes	Yes	N/A	No
P2P based Social Networks	Supports the security requirements for registration and login, access control and secure communication.	Yes	Yes	N/A	No
U-Control	Supports and facilitates digital persona and privacy management (DPPM).	Some	Yes	N/A	No
Privacy Protection issues in SNSs	Classifies users based on their characteristics and helps users determine their required privacy level.	Some	Yes	N/A	No
Reputation Mechanism using SNSs	Includes Automated aid to identify reputation rating based on position in the network structure and provides filtering tool for users' ratings.	Some	Yes	N/A	No
ReDS	Framework for using reputation management to improve the security of locating information in P2P distributed systems. Helps in identifying the reliable local contacts and the malicious nodes.	Some	Yes	N/A	No
Semantic Web Based Framework	Uses Resource Description Framework (RDF) and Web ontology language (OWL) to model SN data into five important aspects of SN sites	Yes	Yes	N/A	No
Re- Socializing Online Social Networks	Decentralized multi-domain SN sites design which complies with user requirements	Some	Yes	N/A	No

not support backup for users' accounts and information.

The semantic Web-based framework [13] uses the Resource Description Framework (RDF) and the Web Ontology Language (OWL) to model SN data into five aspects which are the modeling of personal information, personal relationship, resources, user/resource relationships, and actions. It is a flexible mechanism as not much involvement is required from the users. Information and data are modeled in different classes with different objects and different encryption rules, thus data is protected by the operator itself. Users' data and profile information rely on the existence of the provider.

The Re-Socializing Online SN approach [14] is a novel decentralized multi-domain SN design which complies with user requirements. It is a flexible approach as users have two main schemas to connect with other users which are out-of-band invitation (OOB) and Coupling. All the communications, requests and messages are encrypted with secure message authentication code, so the protection is provided by the operator itself. This approach depends on the provider's existence to make users' data and connections available. Social web space must be always online as social home space and mobile space can not be available permanently. It does not provide backup for the users' information available with the SN service provider.

6. Open Research Issues

The main purpose of SN sites is to facilitate sharing information and contacting people. Therefore, there is a strong need for security mechanisms that operate as part of the SN system to protect and secure user and provider information and activities. Most of the security mechanisms and approaches for SN we studied focus on ensuring the users privacy in SN sites. However; there are other issues that need to be addressed. For example, the proxy-based Real-time protection mechanism needs an additional improvement in terms of updating services and software very rapidly and instantly. In addition, the problem of not giving the control to users over what others reveal about them is still not solved. For example, tagging friends' photos, sharing friends' profiles are options available in some SN sites where friends or other users can simply tag other users in a certain picture or publish their profile without their permission. There are no specific mechanisms or privacy tools which allow users to control what others may reveal about them through these tags or shares. Furthermore, none of the approaches studied or even just mentioned the impact of introducing the security mechanisms on the performance of the system. It is well known that security mechanisms such as encryption, access control enforcement and authentication are compute intensive and requires a lot of resources. In an SN, users are usually in the order of hundreds of thousands and sometimes in millions, executing such mechanisms for all of them will cause huge performance and security problems. Yet, most mechanisms we surveyed did not highlight the tradeoffs between setting higher security measures and the ease of use, performance levels and flexibility to the users.

Moreover, security awareness must be increased among users of all levels by periodically circulating information about SN threats, mechanisms of protection, tools, and user responsibilities. Education is provided by some institutions, but is not taken seriously by governments, academic organizations or SN sites. Moreover, SN sites and their applications do not have the same privacy mechanisms requirements compared to those provided for computer users and mobile users for example. A simple example is controlling who can view a certain piece of information on a users' profile. When accessing the application via computers, users will have the full choice to control who can view the information. However, this option is not provided for mobile SN users. Moreover, some of the challenges that are still facing most of the mechanisms that are trying to protect users' information from the operator; is encrypting images. Most of the mentioned mechanisms provided solutions that encrypt text to be protected from an unauthorized user and the SN provider, but still image encryption was not achieved properly.

7. Conclusion

Social network sites are a major application driver with millions of users all over the world relying on them in keeping contacts and sharing information with others. This huge involvement drives the need for setting the right security measures that help in protecting users' privacy. In this paper, we discussed a number of mechanisms and approaches that help in achieving acceptable levels of security for the SN providers and users. However, many of these mechanisms provided solution for a certain privacy concern but missed others. Moreover when it comes to setting higher security measures it seemed to compromise the usability and flexibility of the system for the average users. However, all surveyed projects failed to mention or measure the tradeoffs between higher security measures and the systems' performance. There are many opportunities for new mechanisms or even existing mechanisms to explore these areas and try to design mechanisms that will not require (or at least minimize) tradeoffs when it comes to users' privacy, information security, usability, flexibility, and performance.

References

[1] Tsai, D.T., A.Y. Chang, , S. Chung, Y.S. Li, "A Proxy-based Real-time Protection Mechanism for Social Networking Sites," in Proc. ICCST 2010.

[2] Graffi, K., P. Mukherjee, B. Menges, D. Hartung, A. Kovacevic, R. Steinmetz, "Practical Security in P2P-based Social Networks," in Proc. IEEE 34th Conference on Local Computer Networks (LCN 2009) Zürich, Switzerland, pp. 269-272, October 2009.

[3] Shin, D., R. Lopes, W. Claycomb, G. Ahn, "A Framework for Enabling User-controlled Persona in Online Social Networks," in 33rd Annual IEEE International Computer Software and Applications Conference, pp. 292–297, 2009.

[4] Ho, A., A. Maiga, E. Aïmeur "Privacy Protection Issues in Social Networking Sites" in proc. AICCSA 2009, p. 271-278, 2009.

[5] Diaz-Sanchez, D., A. Marin, F. Almenarez, A. Cortés, "Social Applications in the Home Network," in IEEE Transactions on Consumer Electronics, Vol. 56, No.1, pp. 220–225, February 2010.

[6] Anderson, J., C. Diaz, J. Bonneau, F. Stajano, "Privacy-Enabling Social Networking Over Untrusted Networks," in Proc. WOSN'09, Barcelona, Spain, August 2009.

[7] Beach, A., M. Gartrell, R. Han "Solutions to Security and Privacy Issues in Mobile Social Networking," in Proc. International Conference on Computational Science and Engineering, p. 1036 – 1042, 2009.

[8] Caceres, R., et al. "Virtual Individual Servers as Privacy-Preserving Proxies for Mobile Devices," In Proc. of MobiHeld'09, 2009.

[9] Luo, W., Q. Xie, and U. Hengartner, "FaceCloak: An Architecture for User Privacy on Social Networking Sites," in Proc. of PASSAT-09, pp. 26-33, August 2009.

[10] Lucas, M. M., N. Borisov, "FlyByNight: Mitigating the Privacy Risks of Social Networking," In Proc. WPES'08, 2008.

[11] Hogg, T., "Security Challenges for Reputation Mechanisms using Online Social Networks," in Proc. AISec'09, pp. 31 – 34, November 2009.

[12] Matthew Wright, Apu Kapadia, Mohan Kumar, and Apurv Dhadphale "ReDS: Reputation for Directory Services in P2P Systems" in CSIIRW '10, Oak Ridge, Tennessee, USA, 21–23 April 2010.

[13] Carminati, B., E. Ferrari, R. Heatherly, M. Kantarcioglu, B. Thurainsingham, "A Semantic Web Based Framework for Social Network Access Control" in Proc. SACMAT'09, pp. 177-186, June 2009.

[14] Durr, M., M. Werner, M. Maier "Re-Socializing Online Social Networks," in Proc. GREENCOM-CPSCOM'10, pp.786- 791, 2010.

[15] Nagy, J., P. Pecho "Social Networks Security," in 3rd International Conf. on Emerging Security Information, Systems and Technologies, pp. 321-325, 2009.

[16] Luo, W., J. Liu, J. Liu, C. Fan, "An Analysis of Security in Social Networks," in Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, p. 648-651, 2009.

[17] Martin, M., M. S. Lam, "Automatic Generation of XSS and SQL Injection Attacks with Goal-Directed Model Checking," the 17th Conference on Security Symposium, 2008.

[18] Sophos,http://www.sophos.com/pressoffice/news/articles/2007/08/ facebook.html. Accessed June 2011.

Racha Ajami is perusing her Ph.D. degree at The Faculty of Information Technology, United Arab Emirates University, UAE. She obtained her B.Sc. in Computer Science from Abu Dhabi University in 2008. Her research interests are in the fields of social networks and e-commerce.

Noha Ramadan is perusing her Ph.D. degree at The Faculty of Information Technology, United Arab Emirates University, UAE. She obtained her B.Sc. in Computer Science from Abu Dhabi University in 2008. Her research interests are in the fields of social networks and e-commerce.

Nader Mohamed is an associate professor at The Faculty of Information Technology, United Arab Emirates University, Al-Ain, UAE. He obtained his Ph.D. in Computer Science from University of Nebraska-Lincoln, Nebraska, USA in 2004. He was an assistant professor of Computer Engineering at Stevens Institute of Technology in New Jersey, USA. His current professional interest focuses on middleware, Internet computing, sensor networks, and cluster, Grid, and cloud computing. He published more than 80 refereed articles in these fields.

Jameela Al-Jaroodi received her Doctorate of Philosophy degree in Computer Science from The University of Nebraska-Lincoln, USA in 2004. Since August 2006, she has been with the Faculty of Information Technology, at The United Arab Emirates University, UAE as an assistant professor. Prior to joining UAEU, Dr. Al-Jaroodi was a research assistant professor at Stevens Institute of Technology in New Jersey, USA. Currently, her research interests involve middleware, distributed collaborative systems, security, and mobile and pervasive computing. While at Stevens, Dr. Al-Jaroodi received the Research Excellence Grant from Sun Microsystems, Inc. In addition, several areas of her research were also supported by the United States National Science Foundation (NSF), Nebraska Foundation, the National Center for Information Technology in Education (NCITE) and UAEU research grants.