LEAF:A Privacy-conscious Social Network-based Intervention Tool for IPV Survivors

Balaji Palanisamy Sheldon Sensenig James Joshi Rose Constantino†

School of Information Sciences, University of Pittsburgh †*School of Nursing, University of Pittsburgh*
{bpalan, sms233, jjoshi, rco100}@pitt.edu

***Abstract*—Destructive relationship behavior directed from one party to another in domestic relationships, both physical and emotional, is a common problem. When the behavior occurs in intimate relationships this is called intimate partner violence (IPV). There are many resources available to survivors of IPV in getting out of abusive situations, but the information is not readily available and is not always easy to find. Furthermore, once the survivor has escaped from the abusive situation, there are not many support type resources that are easily accessible, especially to people lacking transportation and to those residing in rural or suburban areas. LEAF is being created to address the issues that arise from limits in physical community support. The acronym stands for lending encouragement, affirming futures. These embody the vision for a system to provide support to those in difficult situations. The system contains three components: a web portal, a privacy-conscious social network, and a mobile app. By providing a web portal, LEAF aims to be a location where abuse survivors and others can find relevant information. The social network provides an online support community unrestricted by geographical diversity. LEAF incorporates new techniques for anonymous communication in social networks to enable information flow over distributed protected content, while safeguarding both personal information and privacy of individuals from unauthorized disclosure. We believe the outcomes of this system will have the potential for a significant impact on the use of specialized anonymous online social networks in the health care sector including the IPV support system addressed in this work.**

I. Introduction

Social support is an important component of health and well-being throughout life. Online social networks (OSNs) provide a powerful refection of the structure and dynamics of the society of the 21st century and the interaction of the Internet generation with both technology and people. OSNs thus present unprecedented opportunities for social interactions, information sharing and communication for applications in various domains including healthcare (e.g., MedicalMingle [1], PatientsLikeMe [2]), and other applications that have a social dimension. Unfortunately, most existing social networks fail to serve the purpose for people in difficult health situations due to many privacy related concerns related to unstable privacy policies and difficulty in managing personal settings. For people dealing with sensitive issues, such as various diseases, emotional issues, or abuse, the existing OSNs do not meet their need of social support limited to trusted individuals. These people need a system that protects their personal privacy, while allowing them to interact with others that can provide emotional, medical, and physical support. The LEAF system is to fulfill this need. LEAF is being created to address the issues that arise from limits in physical community support. The acronym stands for lending encouragement, affirming futures. These embody the vision for a system to provide support to those in difficult situations.

LEAF is primarily focused on providing a secure privacy-conscious social-network based support system for survivors of intimate partner violence (IPV). We note that destructive relationship behavior directed from one party to another in domestic relationships, both physical and emotional, is a common problem. When the behavior occurs in intimate relationships this is called intimate partner violence. LEAF aims to provide an easily accessible support system to those who have escaped from the abusive situation, especially to people lacking transportation and to those residing in rural or suburban areas.

The privacy-conscious social network is a central part of the LEAF system. In many social communication systems, we find that there is often a loss in privacy in order to accommodate for the required communication trust [6]. Messages in conventional social networks [3], [4], [5] are typically linked with users through friendship relationship in order to obtain higher trust among the communicating entities. In contrast, completely anonymous discussion forums such as [17] present a highly private environment for discussing sensitive topics, however, the increased privacy in these systems comes only at the cost of reduced trust among the communicating parties. The specialized social network in LEAF aims at bringing the best of both the worlds: namely ensuring a highly trusted communication network and at the same time, guaranteeing a high degree of user privacy. The system contains three components: a web portal, a social network, and a mobile app. By providing a web portal, LEAF aims to be a location where abuse survivors and others can find relevant information. The social network provides an online support community unrestricted by geographical diversity. The mobile phone app is to enable users to quickly obtain help if they find themselves in a compromising situation.

The rest of this paper is organized as follows: In Section II we discuss the functional requirements of the LEAF system. In Section III, we present the technical details of the anonymous communication techniques in LEAF. Section IV presents the LEAF platform and implementation. We review the related literature in Section V and we conclude in Section VI.

II. Functional Requirements

This section presents the general architectural requirements as well as the functional requirements of each of the LEAF system components.

A. Architecture

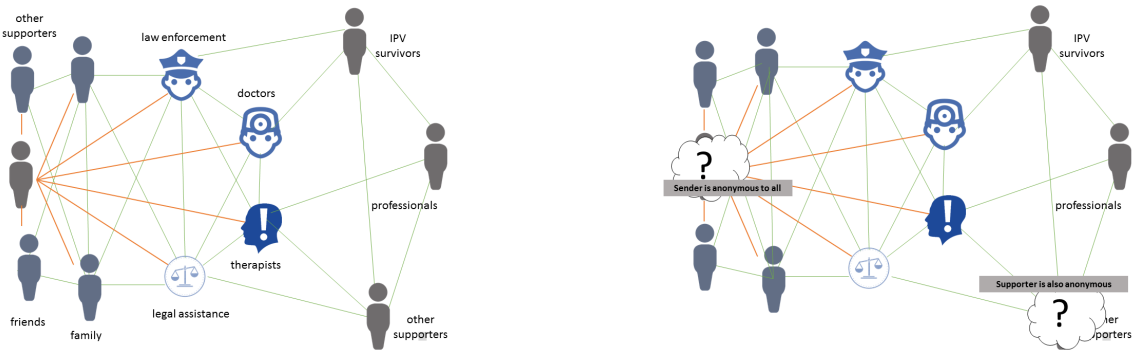
Architectural requirements of LEAF fall into several categories namely security and privacy, administration, and accessibility.

1) Security and Privacy: Security and Privacy is an important requirement of the LEAF system. As users may be in physical danger from abusers, it is necessary to prevent any information that may be used to harm an individual from leaving the system. This includes information on user physical location and contact information as well as any user provided content. Information within the system also must be kept secure. Various content, including user information, must be restricted to certain users.

To prevent Information from leaving LEAF requires secure servers, error free programming, and non-disclosure of data. Server security includes both physically securing access to the hardware and using various security tools to prevent remote access to server content. Non-disclosure of data is a matter of policy. Terms of use for all users should include requiring confidentiality of other user information. It also means that a policy concerning usage of data outside the system (i.e. individual or aggregate data for research, including social network graph structures) must be defined and clearly explained to users. Integrity and availability are addressed internally through the use of access controls and usage limitations. Access controls permit the different types of users to use relevant parts of the system while prohibiting access to all other areas. **Social Network** The LEAF social network is a central part of the LEAF system and its implementation requires user controls, interaction functionality, content controls, and security. One of the key distinguishing features of the LEAF social network is its ability to communicate in a trusted as well as anonymous manner. In many social communication systems, we find that there is often a loss in privacy in order to accommodate for the required communication trust as interactions in real world happen only after the communicating entities identify and establish some trust. Thus the role of trust is fundamental in both social and computing environments and one's privacy can be traded off to gain additional trust to be perceived by the participants. Conventional social network systems [3], [4], [5] that link messages and users through friendship relationships yield higher trust among the communicating users; several privacy attacks that exploit this implicit trust have also been identified [15]. However, as mentioned before, user privacy in these OSNs is traded off for obtaining this increased trust. For instance, each message post and the responses are tagged with the message sender in order to ensure authenticity and trust-worthiness of the information contained in the message. The social network in the LEAF system aims at bringing the best of both the worlds: namely ensuring a highly trusted communication network and at the same time, guaranteeing a high degree of user privacy.

One of the critical requirements in such a system is to anonymize senders, receivers and messages in a privacy-preserving manner so that the information flow in the network simultaneously ensures both information trust and privacy. Note that the IPV survivors may show symptoms of physical wounds, trauma, emotional stress, etc. and may not want to openly participate in interactions and seek intervention or help because of privacy concerns. Thus, a critical requirement here is to possibly allow users to interact anonymously in the online social network. Such an anonymous trusted social network will support the IPV survivors (i) to proactively manage their well-being; e.g., by fostering sharing of experiences among IPV survivors, regular delivery of educational/awareness materials; and (ii) to provide timely intervention in case of impending abuse, or health conditions; such an intervention may include alerting nearby help (e.g., alerting relative/friend/neighbor in the survivor's current city/location). In general, various actors in this system (IPV survivors, care-givers, clinicians, doctors, nurses, social workers and lawyers) may need different types of privacy protection based on their needs. For instance, while some communications require only source anonymity to be protected, some others might require both source and destination anonymity. Similarly, some communications may require only the participants to be private. Accordingly, the privacy requirements can be classified as follows:

- *Protecting source privacy:* Here, the message sender requires her identity to be protected such that it is released either through anonymization or is kept private all the time. For instance, while the sender may allow any friends or friends of friends read her messages, she might require that her identity is kept anonymous and cannot be inferred. A key challenge here is to ensure that the message gets sufficiently anonymized and propagates on the social network with minimal information disclosure. Also, it is critical that the messages are forwarded to the right set of potential participants for the discussion. E.g., the survivor could be interested in anonymously seeking advice from his potential care-givers.
- *Protecting participant privacy:* In addition to sender anonymity required by the sender, in certain scenarios, the participants may require participant anonymity to participate in the discussion. For instance, an IPV survivor may anonymously report an incident among her friends seeking advice from people who have been in similar situations. Such sensitive topics are well responded when the participants are assured of their privacy. In general it is expected that the willingness of participation increases when the system offers higher privacy. Therefore, the goal of the proposed system is to gain more willingness to participate among participants, something similar to completely anonymous systems.
- *Protecting recipient privacy:* Certain situations in OSNs may have a need to even protect the privacy of the recipients of a message. For instance, a care-giver, Tom of an IPV survivor may receive a message from the survivor and may want to forward and ask his friends without being identified that Tom indeed received and forwarded that message. Thus the OSN framework needs the capability to receive and share a message in a completely private manner.
- *Protecting sender and participant location privacy:* When



(a) An example LEAF network

(b) Anonymous communication

Fig. 1: LEAF Social Network

users are mobile, they have an additional need to be able to communicate without exposing their current locations. Users should be able to reach neighboring friends and social workers in a location-aware manner, however, the true locations of the users should not be inferred.

Figure 1(a) shows an example LEAF social network and the anonymous communication is shown in Figure 1(b) where two users communicate without revealing their identities. In general, the survivors of the IPV can significantly benefit with a specialized social network. A main goal of the LEAF social network system will be focused on the intervention and well-being of IPV survivor, allowing survivor to interact with each other, their close friends and care givers (relatives, neighbors, community services, etc.), clinician and doctors, as well as legal entities (e.g., lawyer, police, etc.). To provide better wellness management, we believe OSNs for IPV should be a mediated environment where these various actors can interact to provide, medical, legal and social support. More importantly, propagation of misinformation in IPV OSNs may have severe consequence to patient safety. This precisely calls for an online social network solution that yields both high level of trust as well as privacy.

2) Administration: Administration required for the LEAF system includes managing resources, providing support, performing maintenance and troubleshooting, and enforcing policy. Depending on the system size (depth of content, number of users), this may require coordination of actions between multiple people. Administrators have the ability to configure content and allocate resources. This includes adding to, editing, and deleting web pages and adding groups and subnetworks to the social network. They also can provide support related to managing profiles (including password resets) and pointing users to technical system help. Performance of maintenance and troubleshooting is essential to the health of any system. For LEAF, this includes database management, system auditing, and system cleanup. Regular system auditing is required to monitor for inappropriate behavior, accidental system changes, high resource utilization, and other abnormalities. Policy enforcement is vital to the integrity of the system. Access controls support automatic policy enforcement by helping to prevent violations, but are insufficient to handle actual violations. To remediate violations, administrators can edit and delete user accounts, delete user content, and modify access controls.

3) Accessibility: To promote accessibility of the LEAF system, the website and social network include mobile interfaces and were designed to meet the basics of the Web Content Accessibility Guidelines 2.0 (WCAG2) guidelines [7]. The LEAF website provides pointers to relevant resources, information about the LEAF system, and encouraging stories. Resources include sections where visitors can find listings of local, professional contacts, legal information, and information to assist users in determining what sort of help they need. The website also contains information about the LEAF system and includes encouraging stories. Encouraging stories is meant to be an area to share success stories of people whose lives have improved as a result getting help for abusive relationships. Stories would be added by administrators, but could come from others as well.

In the next section, we introduce the anonymization communication techniques of the LEAF social network.

III. Anonymous Communication in LEAF Social Networks

We propose a set of techniques and anonymization models for supporting anonymous and trusted communication on the LEAF social network. In this section, we introduce the proposed concept of social mixes and illustrate how social mixes would work in an online social network to ensure communication anonymity. We also discuss the key issues of the social mix model including the challenges of attack-resilient social mix construction and route planning.

A. Social Mix model:

We develop the concept of social mix networks which enable hard-to-trace communications among the users in a social network. We define a social mix node as a node (a user in the LEAF social network), which takes in messages from its friends, shuffles them, and forwards them to the next user (possibly another social mix node) until the message reaches the destined user. This approach is inspired from mix networks in anonymous communication systems [18] which breaks the link between the source of the request and the

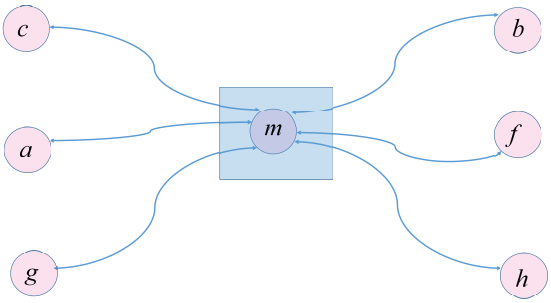


Fig. 2: A Social Mix node

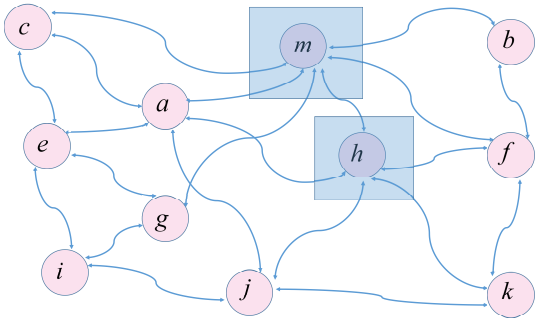


Fig. 3: A Social Mix Network

destination, making it harder for eavesdroppers to trace end-to-end communications. In a similar way, the proposed concept of social mix node tries to ensure anonymity of the message that is propagating in an online social network.

In the proposed social mix networks, mix users only know the user that it immediately received the message from, and the immediate destination to send the shuffled messages to. We illustrate the proposed idea with an example social graph shown in Figure 2, where we construct a social mix at user, m. When a user, say a, wants to anonymously communicate to another user, b, user m can enable this private communication by acting as a social mix node as shown in Figure 3. Depending upon the context, the message sender can choose to hide the message content from the intermediate mix nodes by encrypting them with the public key of the recipient. Concretely, user a prepares a message for user b by appending a random value R to the message, sealing it with the addressee's public key K_b, appending b's address, and then sealing the result with the social mix's public key K_m. Node m opens it with his private key, now he knows b's address, and he sends $K_b(message; R)$ to b. If all but one of the social mix users are compromised by an adversary, untraceability can still be achieved against the attack [18]. The concept of mix networks first described by David Chaum [18] is applied in several network applications including anonymous remailers (such as Mixmaster [19]) and onion routing (including Tor [20]). To the best of our knowledge, the LEAF social network is the first research effort dedicated to developing a mix network model for online social networks addressing the impending needs and challenges of supporting anonymous privacy-preserving trusted communication in OSNs. We illustrate the social mix protocol by continuing on the example shown in Figure 3 where user a communicates anonymously with user b through the social mix m. The message sender uses the social mix's public key (K_m) to encrypt an envelope containing a nested envelope addressed to the recipient, and the social network address of the recipient, b. The nested envelope is encrypted with the public key of the recipient, (K_b) and a social mix typically receives this encrypted envelope and decrypts it using its secret key and finds the address of the recipient (b) with encrypted message bound for b.

Attack Resilient Social Mixing and Route planning: Another challenge in creating and deploying social mixes is that there is often an information flow probability between different social links in a social network due to which some members of the anonymity set in the social mix can be more probable than others. For instance, user Tom may be more willing to share the post of user $Alice$ and respond to him more than user Bob as the friendship link between Tom and $Alice$ could be stronger than that of Tom and Bob. An adversary observing the messages coming in and going out of a social mix can associate the mapping probabilities based on the friendship levels and hence eliminate the low probable members from the anonymity set. However, in a communication network mix, the mix node has complete control on sending the packets on any desired outgoing network link without being constrained by the information flow probability as in the case of social networks. This brings additional challenges in designing an attack-resilient approach to building social mix nodes. In an ideal social mix, given any user in the anonymity set, the adversary has equal probability of associating it with the source of the message and thus the social mix would provide an anonymity equal to the size of the anonymity set. Hence, the uncertainty of an adversary to associate a message source, s to a participating user j is captured by Entropy, $H(s)$ which is the amount of information required to break the anonymity

$$H(s) = -\sum_{j \in A} p_{s \to j} \times log_2(p_{s \to j})$$

where $p_{s \to j}$ denotes the probability of mapping the message source, s with user j. However, in a realistic social mix which is associated with non-uniform information flow probabilities, measuring just the entropy of mix-zone may not be sufficient for an accurate estimate of the achieved user privacy. Our prior work [21], [22], [24] had shown that in order to ensure sufficient mixing quality, it is important to measure the deviation of the mapping probabilities in a pairwise fashion using pairwise entropy: for any two users i and j in the anonymity set, the pairwise entropy for the mapping of a message source s being user j is defined as the entropy obtained by considering i and j to be the only members of the anonymity set. In that case, we have two mapping probabilities: $p_{s \to i}$, corresponding to the probability of mapping s to i and $p_{s \to j}$, corresponding to the probability of mapping s to j. If the probabilities $p_{s \to i}$ and $p_{s \to j}$ are equal, then s is equally likely to be i or j. The attacker has the lowest certainty of linking s to i or j (50%). Formally, let i and j denote the two users in the anonymity set

and s represent the message source, then the pairwise entropy $H_{pair}(i,j)$ between users i and j is defined as follows

$$H_{pair}(i,j) = -(p_{s\to i} log p_{s\to i} + p_{s\to j} log p_{s\to j})$$

A theoretical social mix ensures a uniform distribution for all possible mappings and the highest pairwise entropy of 1.0 for all pairs of users in the anonymity set. We argue that an effective social mix should provide a pairwise entropy close to 1.0 for all possible pairs of users in the anonymity set and the mix construction techniques need to choose the mix node and the inbound and outbound neighbors in such a way that there is a high pairwise entropy among the different users participating in the mix operation.

IV. Platform and Implementation

This section overviews the implementation details of the platform of the LEAF system social network, as well as the main components. We begin by first presenting the implementation details of the LEAF website.

A. Website Implementation

The LEAF website was built from scratch using a basic editor. The website markup and scripting was created using text editors and can be readily modified. Graphics were created using Photoshop CS6. Hosting is currently maintained through web space provided by the University of Pittsburgh. The public-facing LEAF website has been designed for mobile devices, and auto-adjusts for display on tablets and larger screens based on resolution breakpoints. The escape function was implemented to load a decoy browser tab while simultaneously replacing the contents of the original window when invoked. The idea is to provide a cover for users under threat of abuse who may have to explain why they suddenly changed sites when an abuser walks into the room. The functionality has been bound to the 'escape' key on users' keyboards and can also be executed by button click on the site. Functionality is clearly visible on all pages and includes instructions for use. There are limitations to the escape functionality. In Firefox, for example, the pop-up blocker will nix the decoy browser tab if escape is made using the keyboard shortcut. In Chrome, a split-second image of the LEAF website can often be seen when switching from the decoy tab back to the original, site-replaced tab. Other limitations-by-browser may exist that have not yet been identified. Privacy concerns also led to the implementation of cookie-free statefulness and easily opted out geolocation. For cookie-free statefulness, LEAF uses session storage to retain location information. The data is stored client-side, so users can be assured that LEAF does not store or share their location information.

B. Social Network Implementation

In this subsection, we describe the implementation of the LEAF social network. Social networks are complex systems requiring integrated services that range from user security to various methods of member communication. As LEAF is meant to provide support to members revolving around a specific issue and not replace everyday social interaction through different medium, a platform providing moderate functionality is necessary. The platform must provide group functionality and multiple methods of communications, for instance forums and some form of private messaging. To ensure that security and privacy requirements are met, it is necessary to have control of all security mechanisms. As these workings are proprietary in many systems, only open source platforms were considered. This also enables us to remove and add functionality as needed. Five platforms meeting the open source requirement were considered: BuddyPress[8], Diaspora[25], Drupal[9], Elgg[10], and Mahara[11]. Dolphin, which is a popular non-open source implementation that makes source code available with a use license, was also considered in the initial comparison. The concept of modules, existing functionality, and free, open source availability of Drupal and Mahara made them the top platform choices. Both Drupal and Mahara have well organized code, good documentation, and have developers that make patches available on a regular basis. Drupal is primarily a content management system and the core Drupal distribution does not contain any social networking functionality. However, various social networking modules exist and are freely available as open source. Mahara is primarily for online portfolio sharing, but it was implemented as a social network and the portfolio pages could be used for any user content, not just a traditional portfolio. Drupal was chosen for the platform over Mahara based on its extensive documentation, active developer forums, and widespread, varied use. To use Drupal for a social network there are two options: install the core Drupal distribution and add social networking modules or install a pre-built social network distribution. There are several modules related to Organic Groups that adds the desired social networking functionality to the core distribution. Drupal Commons by Acquia is a pre-built distribution that contains the desired functionality and is used by multiple organizations. As Drupal Commons supports the main functional requirements of LEAF, this was chosen as the primary installation.

Drupal Commons requires a MySQL, SQLite or PostgreSQL database, an Apache or Microsoft IIS webserver, and PHP 5.3 or higher. To keep LEAF flexible, Apache was selected as the webserver since it is operating system independent (i.e. it does not require installation on a Windows server). MySQL, SQLite, and PostgreSQL are all free databases. MySQL was selected as Drupal is best integrated with its functionality. Acquia [12] provides limited documentation on their website about Drupal Commons. As it is built around the core Drupal distribution and includes modules from various providers, including Organic Group modules, most of the applicable documentation is on the main Drupal site and the Drupal forums. The actual distribution package may be downloaded either from Acquia or from Drupal's website.

For the social network, the defaults of the selected platform were not sufficient on install to meet the identified requirements. Several existing modules were added, much configuration was done and one new module was created. Most of the required functionality has been implemented by other Drupal users, though not all in the same system. Configuration

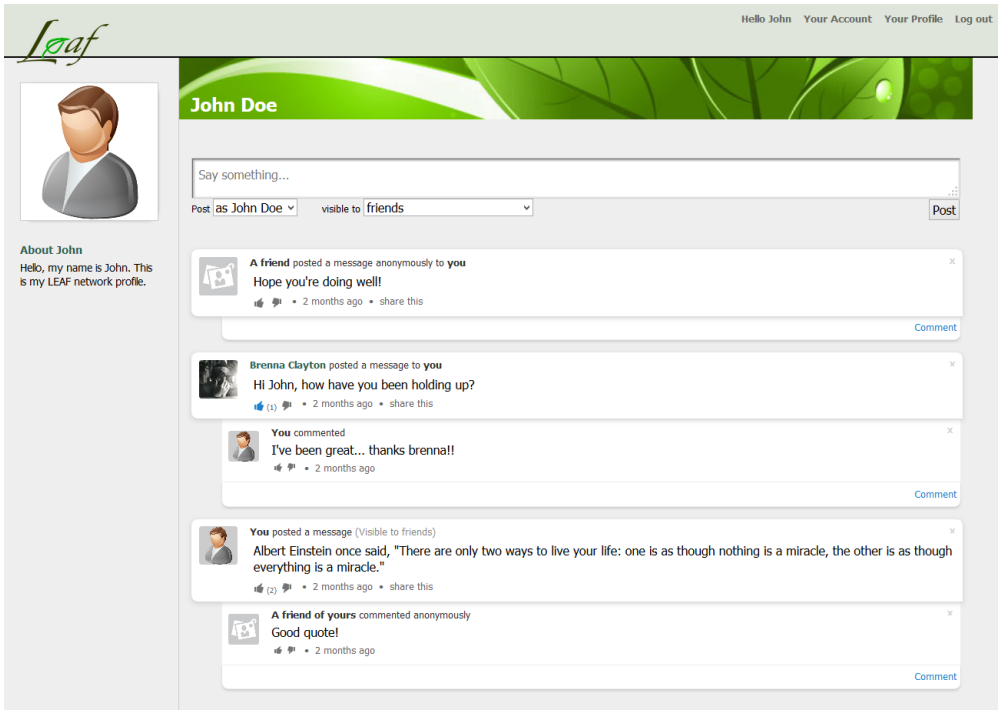
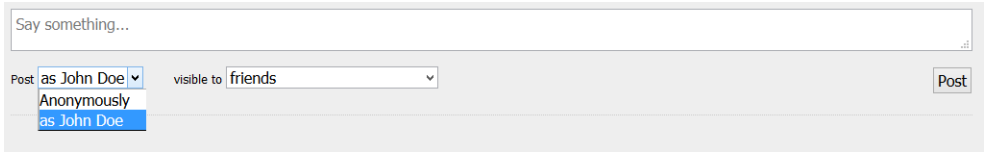
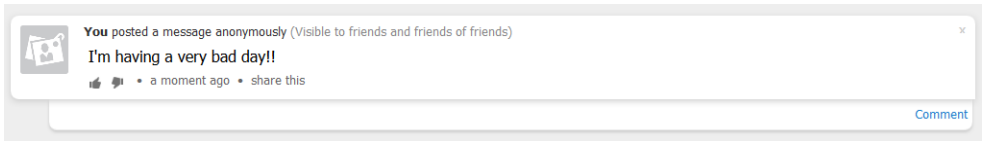


Fig. 4: A LEAF Profile page



(a) Anonymity options when posting



(b) An anonymous post as seen by a friend

Fig. 5: Anonymous Message Post

consisted of changes to the Account settings, DrupalChat, OG field settings, and Search settings, as well as creation of roles. In Account settings, two changes were required. Who can register accounts was changed to ”Administrators only”. This prevents visitors from registering themselves to use the social network. Similarly When cancelling a user account was changed to ”Disable the account and keep its contents”’. This option is necessary to eliminate issues with deleting account contents when the user has created posts or added contents.

In the DrupalChat settings, two changes have been made. First, the public chat room has been disabled. The public chat room would allow anyone to post chat messages visible to all users. Second, the DrupalChat module is able to integrate with the User Relationships module in order to provide the list of visible users. By default all authenticated users will appear in the chat buddy list, but by changing the Relationship Method to User Relationships module, a user will only see, and thus will only be able to chat with, those other users with which he has an established relationship facilitated by the User Relationships module. In OG field settings, the Group visibility field was added to the Group bundle. This enables users to specify whether a group is public or private when creating the group. If a group is private, the group owner (creator) must know a user’s username to add that user to

the group. In Search settings, only Faceted Navigation for Search was selected for Active search modules and the Default search module was set to Faceted navigation for Search. These settings inactivate the regular Drupal User search, which will return all system users, which does not meet the requirements of limiting the other system users that any particular user can view.

Four Drupal roles were created and the default roles, anonymous user and authenticated user, were cleared of permissions as they could not be deleted. The roles are administrator, professional, survivor, and supporter. In addition to the Drupal roles, Organic Group specific roles were configured. The default role named non-user was cleared of all permissions. A group owner role was added to complement the existing member role. These roles can be assigned to group members when they are added to groups. The group creator should assign its own username the group owner role and everyone else the group member role. Permission assignments to roles for both main Drupal roles and Organic Group roles are listed in the Drupal Roles Excel document.

C. Social Network features

Currently, LEAF supports the following social network features.

User Profiles: All non-administrative users of the LEAF social network have profiles. A user's profile represents her presence on the network. In the current implementation, profile details are fairly limited, consisting primarily of a name, profile picture, and a short "About me" section. A user is not required to post a real photo of herself and is not required to use her real name. Similarly, the "About" section is free text which may even be left entirely blank. Since the goal of LEAF is to provide support, users are encouraged to share about their current situation, but no one is forced to share anything beyond what they are comfortable with. An example LEAF profile is shown in Figure 4.

Friends: Users of the system may create friend relationships with other users. This allows users to easily and directly interact with one another. For example, a survivor will add as friends those supporters she has invited to join the network and may wish to add as friends professionals she is acquainted with or who may be local to her area. LEAF builds on top of this concept of friends to include an extended network of users connected through other users (for example, a users extended network includes friends of friends, friends of friends of friends, and so on.)

Self Posts and Wall Posts: In the LEAF social network, there are essentially two types of posts a user can make: a "self-post" or a "wall post". To differentiate, a self-post is a post that a user makes from her own front page or profile page with no specific individual recipient. A wall post on the other hand, is a post which is made by one user to another user's profile. Users may comment on either type of post. When making a post, users may limit the audience to whom the post is visible. For example, a user may wish to share the post with friends only, or perhaps allow the post to be seen by friends and friends of friends, and so on. A user can even allow all LEAF users to view a post even if they are not connected to the poster's extended network.

News Feed and Wall: A user's front page consists of a news feed. This news feed aggregates posts from other users in the network. When post is made that is visible to another user, the post will be visible in that user's news feed.

A "wall" is similar, but is located on a user's profile and displays stories specific to that user. When a user makes a self-post (either from the front page or by posting on his own profile), it appears on his wall as well as in the newsfeed of other users. Similarly, when one user posts to another's profile, that post will appear on the recipient's wall as well as in the news feed of other users.

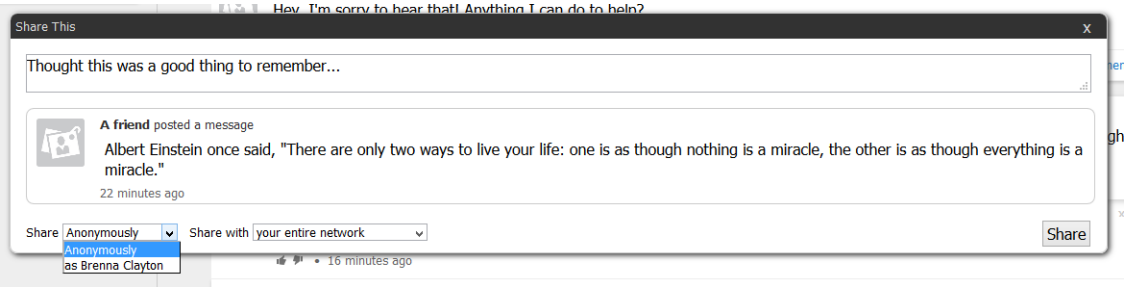
Anonymous Communication features: LEAF supports anonymous communication features to ensure both source and recipient anonymity as well as participation privacy. We briefly discuss them below

Anonymous Posts: In order to facilitate openness and honesty, anonymous communication is a core component of LEAF. Any post made by a user, whether a self-post or a wall post, may be done so anonymously. A typical non-anonymous post will be attributed to the author by labeling it with the author's name, profile picture, and a link to his profile. However, an anonymous post will show a placeholder profile image and merely, in place of a name, the user's relationship to the viewer (i.e., "A friend of a friend posted a message" or "A friend posted a message to you"). Figure 5 shows an example of posting an anonymous message in LEAF.

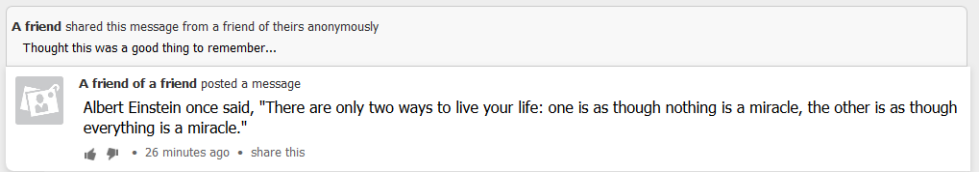
Anonymous commenting: Similarly, when posting a comment, a user may wish to remain anonymous. Again, the commenter's profile picture is obscured and their name is replaced by their relationship to the viewer. In the case of comments, the relationship is also shown between the commenter and the original poster.

Further, any self-post which is anonymous will not be visible on that user's profile.

Anonymous Sharing: Sharing functionality allows a posted message visible to one user to be forwarded to another group of users. In Figure 6, we find how an anonymously shared message from a friend would appear on a user's profile. In LEAF, the sharer may choose whether to be anonymous or not, but the forwarded message will always be anonymous. In this way, a user may share a message with whomever he feels comfortable, and another user may pass the message along without revealing the identity of the original poster. The message is now visible to a much wider audience who may be able to provide helpful comments. In other words, the sharer acts like a social mix providing anonymity of the shared message. A shared post in LEAF will appear on the sharer's wall and in other news feeds as any normal post would. Any comments received on the shared message will be visible to the original poster. Anyone sharing or commenting may remain anonymous to everyone else in the chain. This type of anonymous sharing/forwarding provides a user with a much greater support network than his direct friends. In the current implementation, the selection of social mix nodes (sharers) is done manually and our on-going efforts



(a) Sharing a friend's message anonymously



(b) An anonymously shared message as seen by a friend

Fig. 6: Anonymous Message Sharing

are focused on devising efficient social mix-node selection and message routing planning techniques to ensure automatic sharing of anonymous messages without manual intervention on the LEAF network.

V. Related Work

Ensuring privacy protection in OSNs is an important problem. Existing work had focused from the perspectives of access control [13], [14] and other friendship-based privacy attacks [15], [16]. While there is significant ongoing research activities addressing various security and privacy challenges in OSNs, one issue that has not been addressed adequately is that of the varying levels of anonymity that different participants may need when they interact within a social network. Outside of online social networks, there had been work on anonymous communication services such as AnonymousSpeech [17] that enable private communication to the participants. The concept of anonymous mix networks was first described by David Chaum [18] in 1981 and had been applied in several domains including anonymized network communication systems such as Tor [20]. However these systems do not provide a friendship-preserving communication model and therefore lack the inherent communication trust that OSNs offer.

There had been recent work on decentralized social network systems with the goal of providing higher confidentiality to users' data. Diaspora [25] is a social network that users install on their own personal web servers, without support for encryption. PeerSon [27], LotusNet [29] and Safebook [28] are distributed OSNs that benefit from DHTs in their architecture. These research efforts focused on the scalability and performance aspect of decentralized models and in some cases the confidentiality of the stored data. However, they do not consider ensuring communication privacy and sender/recipient anonymity which is the focus of the social network in LEAF. To the best of our knowledge, the social network presented in LEAF is the first research effort dedicated to developing an anonymous communication mechanism over online social networks.

VI. Conclusion

The emergence and popularity of online social networks in recent years has changed the Internet ecosystem leading to a more collaborative environment. The focus of the LEAF project is to design and build a privacy-preserving OSN framework that enables trusted anonymous communication to the survivors of IPV and the social actors in the support system. While there are significant ongoing research efforts addressing various security and privacy challenges in OSNs, one key issue that has not been addressed adequately is that of the varying levels of anonymity that different participants may need when they interact within a social network. Such a need specifically arises in the LEAF social network that focuses on specific types of issues related to supporting survivors of Intimate Partner Violence (IPV) where a survivor may want to communicate with several social actors. We presented the first prototype of the LEAF system that supports privacy-preserving communication among its users and ensures a secure and a trust-worthy online communication forum for intervening and supporting survivors of IPV. Our ongoing and future work is focused along two dimensions: first, we are continuing research on the theory and algorithms of deploying attack-resilient social mix nodes and anonymous message route planning techniques in social networks and second, we are pursuing clinical studies to evaluate the efficacy and effectiveness of LEAF in intervening and supporting the actual survivors of IPV.

VII. Acknowledgements

Support for this research has been provided by NSF DGE Award #1027167. Sheldon Sensenig has been supported by the SFS scholarship program. Besides Sheldon Sensenig, other students supported by the SFS program have also contributed to the development of the LEAF website.

References

[1] Medical Mingle: http://www.medicalmingle.com/
[2] Patients Like Me: http://www.patientslikeme.com/
[3] Facebook: https://www.facebook.com/
[4] Twitter: https://twitter.com/
[5] LinkedIn: https://www.linkedin.com/
[6] C. Zhang, J. Sun, X. Zhu, Y. Fang Privacy and Security for Online Social Networks: Challenges and Opportunities. In *IEEE Network*, 2010

[7] Web Accessibility Initiative- WCAG 2 at a glance, USA. *http://www.w3.org/WAI/WCAG20/glance/Overview.html*
[8] Buddypress: http://buddypress.org/
[9] Drupal: http://buddypress.org/
[10] Elgg: http://elgg.org/
[11] Mahara: https://mahara.org/
[12] Acquia: https://mahara.org/
[13] B. Carminati, E. Ferrari, A. Perego Enforcing access control in Web-based social networks. In *ACM Transactions on Information and System Security (TISSEC)*, 2009
[14] S. Jahid, P. Mittal, N. Borisov EASiER: encryption-based access control in social networks with efficient revocation. In *ASIACCS*, 2011.
[15] L. Jin, H. Takabi and J. Joshi Towards Active Detection of Identity Clone Attacks on Online Social Networks In *CODASPY*, 2011.
[16] L. Jin, J. Joshi, M. Anwar Mutual-friend Based Attacks in Social Network Systems. In *Computer & Security*, 2013.
[17] https://www.anonymousspeech.com/
[18] D. Chaum Untracable electronic mail, return addresses, and digital pseudonyms. In *Communications of the ACM,* 1981
[19] Mixmaster: *http://en.wikipedia.org/wiki/Mixmaster_anonymous_remailer*.
[20] https://www.torproject.org/
[21] B. Palanisamy and L. Liu. MobiMix: Protecting Location Privacy with Mix-zones over Road Network. In *ICDE*, 2011.
[22] B. Palanisamy, L. Liu, K. Lee, S. Meng, Y. Tang and Y. Zhou Anonymizing Continuous Queries with Delay-tolerant Mix-zones over Road Networks. In *DAPD*, 2014.
[23] B. Palanisamy and L. Liu Effective Mix-zone Anonymization for Mobile Travelers In *Geoinformatica*, 2014.
[24] B. Palanisamy and L. Liu Attack-resilient Mix-zones over Road Networks: Architecture and Algorithms In *IEEE TMC*, 2014.
[25] Diaspora: http://en.wikipedia.org/wiki/Diaspora_(social_network)
[26] M. Backes, M. Maffei, and K. Pecina A security API for distributed social networks In *NDSS*, 2011.
[27] S. Buchegger, D. Schioberg, L. H. Vu, and A. Datta PeerSoN: P2P social networking early experiences and insights. In *SNS*, 2009.
[28] L. A. Cutillo, R. Molva, and T. Strufe Safebook: Feasibility of transitive cooperation for privacy on a decentralized social network In WOWMOM, 2009
[29] L. Aiello and G. Ruffo LotusNet: tunable privacy for distributed online social network services In *Computer Communications*, 2012.