International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 6 (July 2014) http://ijirae.com

Privacy Perspectives, Requirements and Design trade-offs of Encounter- based Social Network

Ramya S[1], Shruthi J[2], Bharathi R[3], Ambika G N[4], Chinnaswamy C N[5].

[1] *Research Scholar, M.Tech CNE(PT), Dept. of PGSCEA, NIE, Mysore*
[2] *Asst. Prof, Dept. of Computer Science and Engineering, BMSIT, Bangalore*
[3] *Assoc. Prof, Dept. of Computer Science and Engineering, BMSIT, Bangalore*
[4] *Asst. Prof, Dept. of Computer Science and Engineering, BMSIT, Bangalore*
[5] *Assoc. Prof., Dept. of Information Science & Engineering, NIE, Mysore*

ABSTRACT -- Encounter-based social networks link users who share a location at the same time, as opposed to the traditional social network model of linking users who have an offline friendship. Privacy is one of the friction points that emerge when communications get mediated in Encounter-based Social Networks. Different communities of computer science researchers have framed the 'Online Social Network privacy problem' as one of surveillance, institutional or social privacy. In this article, we first provide an introduction to the surveillance, social and institutional privacy perspectives. We then explore the differences between these approaches in order to understand their complementarity. In this paper, we explore the privacy requirements for Encounter-based social networks. We provide an overview on the privacy guarantees and feasibility of SMILE and also its drawback in meeting certain requirements.

Key Words: Encounter-Based Social Networks, OSNs, Privacy, PETs, Authenticity, Requirements, SMILE.

1. Introduction

In the traditional model of social networks, users choose their contacts from a set of off-line relations. Regardless of their service, these usual networks support only a subset of social networking: two users will only be able to establish an association in the social network if they know each other, or are introduced to each other. Whereas, in an encounter-based social network, the only requirement for establishing a link is to be in the same place at the same time—similar to starting up a conversation at a public place. Encounter-based social networks would provide a computing infrastructure to allow for making of varied services such as a "missed connections" virtual bulletin board, on-the-fly introductions (business card exchange).

Encounter-based social network is an online social network. Researchers from different sub-disciplines in computer science have identified some of the problems that arise in OSNs and projected a various range of "privacy solutions". one of the intentions of this paper is to put these approaches of privacy into perspective.

Privacy problems can be distinguished into three types. The first approach concentrates on the "Supervision problem" that arises when the personal information and social interactions of OSN users are leveraged by governments and service providers. The second approach deal with those problems that emerge through the necessary arbitration of boundaries of social interactions getting mediated by OSN services, in short called "social privacy". The third approach deal with problems related to users losing control and lapse over the collection and processing of their information in OSNs, also known as "institutional privacy"[6].

Although encounter-based systems appear very analogous to existing social networks, they present a considerably different set of challenges, out of which are security and privacy of users and authenticity of the other party in a conversation are important. Assurances that are trivial in traditional social networks, such as authenticity (ensuring one is communicating with the desired person), become unwrapped problems in encounter-based networks. Additionally, requirements like obscurity—a feature that is not needed in most usual online social networks based on prior face-to-face contact—need to be considered in encounter-based networks. This is desirable because users would look forward for information about people they happen to meet to stay private. Also, since people do not automatically place their faith in others simply based on presence in the same location, it is also desirable to *disclose the minimum amount of information required* for future secure communication. Sharing complete personal information is not the primary goal of encounter-based networks, but can of-course be easily put into practice if both users agree upon the successful verified encounter.

2. The three Perspectives for Online Social Network

A. *The Supervision/Surveillance perspective*

1. OSNs have acquired significance beyond the "social", as a site for citizens to contest their ruling institutions. 2. Same institutions will attempt to instrumentalize OSNs to monitor and intervene in the lives of their citizens. These two uses, the nations' use of OSNs for democratic liberation and state institutions' reflex to monitor and influence those citizens, are in tension. In that sense, they render a very typical definition of privacy relevant in the context of OSNs: privacy as a right that citizens can invoke to protect themselves from an overbearing surveillant state.

In order to overcome surveillance privacy problem , it is necessary for state institutions assert such power in collaboration with private organizations, constituting what some authors call the "surveillant assemblage"[1]. This is exactly the type of surveillance that occurs when law enforcement and intelligence agencies around the world start acting in concert with OSN providers. Further 'silently' conducting surveillance, these assemblages may proceed to limit free speech, e.g., censor user content or groups in OSNs. In other instances, state actors in alliance with Internet Service Providers (ISPs) block OSN sites. This exercise, which has become common in situations of civil unrest, aims to avoid citizens from leveraging OSNs to self-organize or share and access information.

The set of technologies that we refer to as "Privacy Enhancing Technologies" (PETs) grew out of cryptography and computer security research, and are thus intended following security engineering principles, such as threat modelling and security analysis. Traditional security technologies were developed for national security purposes, and later, for securing commercial information and transactions. They were meant to shield state and corporate secrets, and to safeguard organizational operations from interference. The privacy problems addressed by PETs are in many ways a reformulation of old security threats, such as confidentiality infringes or denial of service attacks. This time however, ordinary citizens are the intended users of the technologies, and surveillant assemblages are the threatening entities from which they need protection. Unsurprisingly, the typical user and use of PETs is the 'activist' engaged in political dissent. The goal of PETs in the environment of OSNs is to enable folks to connect with others, share, access and publish information online, free from surveillance and intervention. Ideally, only information that a user explicitly shares is available to her intended recipients, while the disclosure of any other information to any other parties is prevented. Furthermore, PETs aim to improve the ability of a user to publish and access information on OSNs by providing her with means to circumvent censorship.

B. ***The Social Privacy perspective***

In contrast to the surveillance perspective, when mainstream media account on privacy violations in "everyday life", they do not frame OSNs as incubators of social revolution, but as consumer goods. The users are thus "consumers" of these services. They spend time in these (semi-)public spaces in order to mingle with family and friends, get access to information and discussions, and to spread out matters of the heart as well as those of belonging. That these activities are made public to 'friends' or greater audiences are seen as a crucial component of OSNs. However, it is important that disclosures, and the interactions that follow, happen at the users' discretion. Otherwise users can be subject to "unexpected" and "regrettable" interactions with friends, family and employers.

Popular accounts of privacy breaches in news media have made this social privacy problem evident: partners finding out about wedding rings before the official proposal, employer's learning about untrustworthy sick leaves, tax authorities finding out about undeclared expensive purchases, and families noticing the sexual preferences of their children.

These privacy problems have been studied by a variety of research communities within and beyond computer science. Researchers have shown that the way clearness, sharing and
friending is embedded into OSN design plays an important role in the way information flows in these networked systems . These novel flows of information may undermine the spatial
may be disrupted while new ones may come into being. These may be limitations between the private and the public, the cherished and the distant, openness and closeness as well as the self and others . For example, a casual status update on an OSN may start
living a life of its own. With one click, a user may contact a remarkable audience, while she may neither determine its size nor its geographic distribution. The reach of the status update may not only depend on her: her friends may decide to 'share' it further with others in their networks. Multiple copies of the update may hence exist much longer than the intended conversation blurb.

Social privacy relay to the concerns that users raise and to the harms that they experience when technologically reconciled communications disturb social boundaries. Several research studies show that OSN users struggle with a variety of related issues: damaged reputations, interpersonal divergence, presentation anxiety, unwanted contacts, context collision, annoyance, peer pressure, blackmailing, and the list continues. Further, enabling privacy practices through design requires expanding the focus from individual actions to include collective dynamics, and provisioning with the online-offline divide.

An important body of work dealing with social privacy problems in OSNs comes from the HCI and Access Control communities. Research in HCI, often informed by behavioural economics, focuses on transparency and feedback solutions. The intention is to develop design principles that aid individual users in making better privacy decisions and hence improving collective privacy practices. In Access Control, solutions that utilize methods from user modelling aim to develop "meaningful" privacy settings that are intuitive to use, and that contribute to users' information management needs.

C ***The Institutional Privacy Perspective.***

Institutional privacy solutions the service provider is trusted and law enforcement is a legitimate stakeholder. Institutional privacy provides organization-centric solutions. Research on institutional privacy is aligned with regulatory approaches to privacy, e.g., the Fair Information Practice Principles (FIPPs) recommended by the Federal Trade Commission (FTC) and the EU Data Protection Directive (EU DPD). Both FIPPs and the EU DPD strive to balance organizational and individual needs in data collection and processing: organizations should be able to collect process and share personal data, and they should offer users with

some transparency and control over the same – with a number of exceptions, e.g., for law enforcement. Computer science research on institutional privacy studies ways of improving organizational data management practices for compliance, e.g., by developing means for information flow control and accountability in the back end.

3. Requirements and Challenges faced in Encounter Based Social Networks

Many encounter-based designs do not even consider basic security and privacy requirements along with functionality and performance. Others dont succeed to meet these requirements even though they were created with the precise goal of satisfying them. Below, we explore some requirements for idealized secure encounter-based social networks. While this list is by no means complete, it can be used as a preliminary guide for assessing past and future designs.

3.1 Security Requirements

We outline some of the required security features of encounter-based social networks. Note that these requirements are nonspecific in the sense that they may apply to *many distributed systems* which combine human interaction, sensitive private information, and network communication. The security requirements we expect in these systems are as follows.

(*i*) P*rivacy* or *unlinkability*. The privacy of two parties sharing an encounter must be protected, even from others in the locality who may also take part in concurrent encounters. In this case, privacy means that an external adversary (even one taking part in the encounter or colluding with a "bulletin board" or rendezvous server to be used in latter phase) who is not one of the two users of interest should not be able to conclusively determine that two users have made a connection.

(*ii*) *Authenticity*, meaning that when two users decide to make a connection, they should be guaranteed that messages indeed originate from each other.

(*iii*) *Confidentiality*, meaning that information exchanged between two users should be accessible only to them.

3.2 Functional Requirements

The following are nonspecific functional requirements in the context of large-scale distributed systems that are also desirable for an encounter-based social network.

(*i*) *Availability*. As such, the infrastructure to exchange encounter information should be accessible *most of the time*. The unavailability of individual users should not affect the availability of other users. Since the time at which encounter parties check for potential encounters associated with their activities could be random, the encounter-based social network is more sensitive to availability than conventional social networks.

(*ii*) *Scalability*. With typical social networks being large in size, any potential social network design, including those based on encounters, should scale to support a large number of simultaneous users. This requires minimizing dependence on a centralized entity.

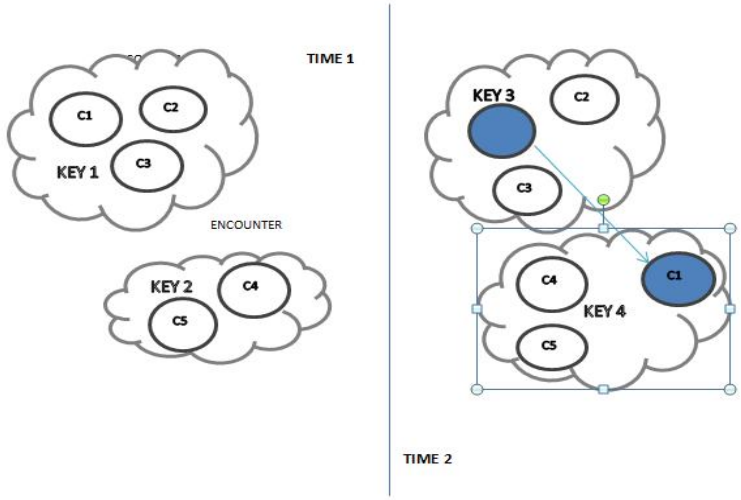

Figure 1: Encounter Key Distribution

4. SMILE

Some of the above requirements are met by SMILE [5]. SMILE is a mobile social service in which trust is established solely on the basis of shared encounters; the service provider is not trusted to access users' location information and we assume no pre-established trust relationships among users. In SMILE, users who want to communicate with each other must prove that an encounter occurred between them. The first device in the encounter generates and broadcasts the "encounter key" to other devices within its communication range.

Then the same device posts a cryptographically-secure hash of the encounter key, along with a message encrypted using the encounter key to a centralized server. Due to the pre-image resistance properties of the hash function, the centralized server will not be able to recover the encounter key without help, and therefore cannot read the message. Other users of SMILE having the same encounter key may claim the encounter by looking up the key hash , which is used for indexing the encrypted message at the centralized server.

The users with the correct key will be able to decrypt the message left by the first encounter party at the server, and every user with the correct key be able to derive the hash value for retrieval. The benefits of the basic design of SMILE as it is illustrated here is that it reduces the misuse in the encounter system: only people who have been at the encounter place are those who know the encounter credentials and are able to claim the encounter. Encounter key distribution is depicted in *Figure1*. In addition to the basic design, SMILE tries to provide two features: k-anonymity and decentralization. K-anonymity is achieved by truncating the hash values of the keys so that a single user is concealed amongst k other users with the same truncated value. SMILE characterizes a decentralized system that uses anonymizing networks of re-mailers for communication, claiming to provide k-anonymity by requiring each user to have at least k identifiers. SMILE allows strangers who shared an encounter in the past to communicate at a later point in time. An encounter is defined as two people being in close physical proximity to each other for a period of time.

- ***Drawbacks of SMILE***

The system's availability and scalability are limited, *as the system depends on a centralized server that is easy to interrupt— a problem that is not unique to* SMILE*, but to a certain extent any design that uses a centralized online entity*. Furthermore, the claimed security guarantees might not meet the requirements described above. As the confidentiality of encounter- related information is safeguarded by encryption, the privacy of users in SMILE can be infringed. In principle, while the problem exists in systems that rely on a centralized server, one can enhance the performance of SMILE and alleviate the problem by providing a server with high availability guarantees, which arrive at cost that need to be considered as part of the design.

First, SMILE is prone to an *impersonation attack* performed by a user present during the encounter. As no authentication is done during key agreement, any user can snoop on the encounter information and later claim to be the party involved in encounter. This attack can further be extended to monitoring: if the adversary exchanges keys with the first user pretending to be the second, and repeats this with the other user, the adversary can carry out a Man in the Middle attack and monitor all messages passed between users.

Second, SMILE is prone to *user collusion[3]*, an attack that was formerly reported in social interactions , a few malicious users colluding with the rendezvous server may gain enough information about activities of other honest users (such as timestamps, locations information, and encounter keys) for the server to unmask users, determining the identities of communicating parties.

Finally, while not particularly a specific problem of SMILE but every system using such a building block, the k-anonymity in SMILE requires that each user know the number of other nearby SMILE users in order to make sure that there are enough people around to mask the activity of an individual— that the user is indistinguishable from k others in a given encounter setting. This, however, can be easily changed by a Sybil attack[2] where a single adversary pretends to be $k - 1$ other SMILE users, *compromising truthful user's anonymity*.

5 Conclusion

We made some attempts at identifying Surveillance, Social and institutional privacy problems. Then we outline several requirements that ideal encounter-based social networks need to satisfy. We have provided an overview on the privacy guarantees and feasibility of SMILE and also its drawback in meeting certain requirements.

REFERNCES

1. Kevin D. Haggerty and Richard V. Ericson. "The Surveillant Assemblage". British Journal of Sociology, 51(4):605 – 622, 2000.
2. J. Douceur. The sybil attack. *P2P Systems*, pages 251–260, 2002.
3. M. Macy. Learning to cooperate: Stochastic and tacit collusion in social exchange. *The America Journal of Sociology*, 97(3):808–843, 1991.
4. Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. IEEE Security and Privacy, 3(1):26 – 33, January/February 2005.
5. Justin Manweiler, Ryan Scudellari and Landon P. Cox " SMILE: Encounter-Based Trust for Mobile Social Services," 2011.
6. Kate Raynes-Goldie. "Privacy in the Age of facebook: Discourse, Architecture, Consequences." PhD thesis, Curtin University, 2012.
7. Qi Xie and Urs Hengartner, "Privacy-Preserving Matchmaking For Mobile Social Networking Secure Against Malicious Users" Ninth Annual International Conference on Privacy, Security and Trust, 2011
8. E. De Cristofaro, C. Soriente, G. Tsudik, and A. Williams. Hummingbird: Privacy at the time of twitter. In IEEE Symposium on Security and Privacy, pages 285–299. IEEE Computer Society, 2012.

