Social privacy score through vulnerability contagion process

Aghiles Djoudi ‡ ⋆, Rafik Zitouni‡ and Laurent George⋆
ECE Paris‡, SIC Laboratory, 37 Quai de Grenelle, 75015 Paris, France
LIGM/ESIEE Paris⋆, 5 boulevard Descartes, Cité Descartes, Champs-sur-Marne, France
Email: aghilesdjoudi@gmail.com, rafik.zitouni@ece.fr, laurent.george@esiee.fr

Abstract—The exponential usage of messaging services for communication raises many questions in privacy fields. Privacy issues in such services are strongly related to the graph-theoretical properties of users' interactions representing the real friendships between users. One of the most important issues of privacy is that users may disclose information of other users beyond the scope of their interaction, without realizing that such information could be aggregated to reveal sensitive information. Determining vulnerable interactions from non-vulnerable ones is difficult due to the lack of awareness mechanisms.

To address this problem, we analyze the topological trust relationships between users to notify each of them about their vulnerable social interactions. Particularly, we analyze the impact of trusting vulnerable friends in affecting other users' privacy concerns by modeling a new vulnerability diffusion process. Simulation results show that over-trusting vulnerable users speeds the vulnerability diffusion process through the network. Furthermore, vulnerable users with high reputation level spread their vulnerability widely trough the network, this means that the vulnerability diffusion process affects the biggest number of users when vulnerable users get a high level of trust from their interlocutors. This work contributes to the development of privacy awareness framework that can alert users of the potential private information leakages in their communications.

Index Terms—Vulnerability measurement, Messaging services, Security, Privacy.

I. Introduction

With increasing frequency, communication between citizens and institutions occurs via some type of e-mechanisms, such as websites, email, and social media. In particular, email platforms are widely being adopted because of their simplicity of use. Due to the social aspect of these mechanisms, users are continuously affected by their friends' privacy vulnerability. Users can take all the required measures to protect themselves from potential information leakage, but if their friends didn't respect the same measures, this indirectly harms their privacy concerns, especially when they grant a high-level of trust to them.

Currently, available solutions address the privacy issues of users by measuring their vulnerability toward active attackers in low layer protocols (e.g. HTTPS, SSL, PGP, IPsec, etc), or by suggesting new privacy policy settings of their applications. These works are efficient to protect users from external vulnerabilities, but they appear very weak to protect users from (legitimate) information leakage between messaging services users. Many other works, for example liu_framework_2010 address this problem by measuring the users' privacy vulnerability individually without caring about the social context of the problem. Few works zeng_trustaware_2014 b.s._privacy_2015 address this problem from a topological view of users' relationships during their social interactions. Our work is motivated by the potential of privacy awareness frameworks to help users being conscious about the trustworthiness of their social interactions.

Trust networks allow users to rate other users, they can put their level of trust in their interlocutors based on their own beliefs such as "Alice trust Bob as 0.8 in [0,1]" massa_trustaware_2007 Trust statements can then be aggregated in a single trust network representing the relationships between users massa_trustaware_2007 Trust metrics in our work are related to the relation strength between users such as the frequency of interactions, common interests, common friends, etc. Trust metrics can also be related to the relationship closeness such as family, friends, colleagues or just unknown. Based on such metrics and the topology of the interaction network, the system can suggest how many users are trustworthy based on different opinions of interlocutors, this suggestion represents their reputation.

Trust and reputation metrics are used in our work in order to study the relationship between them and users' privacy vulnerability. Reputation concept refers to the extent to which a user is trustworthy. This means that he plays a central role in preserving or revealing sensitive information of his interlocutors. Reputation system collects, distributes and aggregates feedback about participants' past behavior to allow users decide whom to trust and with whom to exchange sensitive information, users could then decide to not interact with those who are vulnerable to preserve their own privacy.

Messaging services users often exchange messages with a high number of users without caring about the vulnerability of their social environment. In this paper, we deal with privacy issues by studying the impact of trust in preserving privacy.

The remainder of this paper is organized as follows. Section II elucidates summary of related works. In Section IV,

we propose our vulnerability contagion process to reveal the social vulnerability of users. Our experimentation with Enron dataset and our findings are presented in Section V and VI respectively. Finally, conclusion and future works are drawn in Section VII.

II. Related work

To evaluate the privacy risk of social network users, trust metrics are used to measure the extent to which users can be trusted. Trust metrics can be classified into two main categories: global and local trust metrics. Local trust metrics compute trust values that are dependent on the target user. They take into account the very personal and subjective views of the users. They predict different values of trust for every single user based on their own experience. Global trust metrics, on the other hand, predict a global reputation value for each node, based on both the experience of all other users and the topology of the social network.

Much work has focused on adapting existing privacy settings to the users profile, for example, the machine learning techniques used in Protect_U gandouz_protect_2012 allow recommending privacy settings based on trustworthy friends. Protect_U analyzes the existing privacy settings and ranks them under four risk levels: Low Risk, Medium Risk, Risky and Critical. The system then suggests personalized recommendations to allow users to make their accounts safer. In order to achieve this, it draws upon two protection models: local and community-based. The first model uses the visibility of users profile information to suggest recommendations. The second model searches trustworthy friends to encourage them to help improve the safety of their friends account.

Despite a large amount of work on social trust, a decentralized interest-based marketplace is built for the first time in SocialMarket frey_social_2011 authors of this framework propose the use of trust relationships to build their decentralized interest-based marketplace. In contrast, TAPE framework developed by Zeng et al. yongbozeng_study_2015 tried to solve the privacy quantification problem gundecha_exploiting_2011 from a different angle. First, they calculate the privacy trust score of each user to know how likely a friend could reveal or preserve others' personal information. Next, they propose an information diffusion process fang_privacy_2010 The most important contribution made by TAPE framework yongbozeng_study_2015 is in considering information diffusion to reveal privacy leakage in communication.

Zeng and Xing zeng_trustaware_2014 studied the maximization of users relationships by making trustful friends without leaking their private information to unwanted parties. The authors propose a security risk estimation framework to deal with such a problem. The framework proposed is composed of two parts, the calculation of Individual Privacy Leakage Probability (IPLP) and the Relationship Privacy Leakage Probability (RPLP). Two vectors namely privacy protection awareness (PPA) and privacy protection trust (PPT) are proposed in this paper to estimate IPLP.

Gundecha et al. gundecha_exploiting_2011 propose an advantageous approach to the problem of identifying a user's vulnerable friends. The approach proposed differs from existing work by integrating a vulnerability-centered approach. On most online social networks (OSN), a mole of work addressed the problem of protecting user's individual attributes only, however, few works address the problem of protecting users relationships from vulnerable friends.

Another example that consolidates our intention to build our privacy awareness framework is called LENS hameed_lens_2011 Hameed hameed_lens_2011 proposed a novel spam protection system that maximizes the number of trusted nodes who send only trusted emails, only emails to a node that have been allowed by these trusted nodes can be sent through the network. The authors proposed using trust and reputation systems to detect whether a user is trustful or not.

SocialEmail tran_social_2010 is a trust by design communication system, it considers trust as an integral part of the communication system. SocialEmail rank trust paths to rate the messages, these last ones are routed through existing friendship links that are weighted with different trust level. This gives each email recipient an overview of the trustworthiness of path taken by a message to reach him. In contrast, such methods are not sufficiently effective in dealing with legitimate emails from senders outside SocialEmail.

Social interactions allow users exchanging messages with other users easily and quickly. xiang et al. xiang_modeling_2010 proposed a social interaction as an indicator of interpersonal tie strength. As a consequence, an unsupervised model has been developed to estimate the relationship strength from their interaction activity xiang_modeling_2010 Such methods could extract the level of trust between interlocutors based on the relationship strength between them. However, this application is not designed to be automated, users must manually score other users, score messages or create whitelists.

Vidyalakshmi et al. b.s._privacy_2015 proposed a privacy control framework for information dispersal on social networks, they use the quadratic form of bezier curve to arrive at privacy scores for friends, they use the communication information for pre-sorting friends which is lacking in vidyalakshmi_privacy_2015 Similarly, Akcora et al. akcora_risks_2012 develop a graph-based approach and a risk model to learn risk labels of strangers, the intuition of such an approach is that risky strangers are more likely to violate privacy constraints.

Privacy Index (PIDX) proposed in nepali_sonet_2013 is a measure of a user's privacy exposure in a social network. PIDX is a numerical value between 0 and 100 with a high value indicating high privacy risk in social networks. An attribute's privacy impact factor is a ratio

of its privacy impact to full privacy disclosure. Thus, an attribute's privacy impact has a value between 0 and 1. They consider the privacy impact factor for full privacy disclosure is 1.

Fang and Le Fevre fang_privacy_2010 proposed a Privacy Wizard to help users grant privileges to their friends. It automatically configures users' privacy settings. The wizard asks users to first assign trust labels to selected friends. The wizard is then training to classify tagged friends based on both profile information and labels assigned by users themselves. Ones this step is finished, the wizard is now able to assign new labels to unlabeled friends based only on their profile information. In a similar way, some studies maximilien_privacyasaservice_2009 propose a methodology to quantify the vulnerability of user's privacy settings. A risk score reveals to users how far their privacy settings are from those of other users. However, it does not help users refine their settings in order to achieve a more acceptable configuration.

Abdul-Rahman and Hailes abdul-rahman_supporting_2000 proposed a trust model with virtual communities and artificial autonomous agents. The model defines a direct trust and a recommender trust. Trust can only have discrete labeled values, namely Very Trustworthy, Trustworthy, Untrustworthy, and, Very Untrustworthy for direct trust, and Very good, good, bad and, very bad for recommender trust. The difference between the two ratings from different entities can be computed as a semantic distance that can be used to adjust further recommendations. The combination of ratings is done as a weighted sum, where the weights depend on the recommender trust.

All previous work didn't take into consideration the topological aspect of interactions to measure social vulnerabilities of users. The closest study to our approach is that presented in zeng_trustaware_2014 However, this solution doesn't study the impact of having interactions with vulnerable users. In this paper, we study the impact of trusting vulnerable users in preserving the privacy of all users in the communication network.

III. Related work

To evaluate the privacy risk of social network users, trust metrics are used to measure the extent to which users can be trusted. Trust metrics can be classified into two main categories: global and local trust metrics.

Local trust metrics, compute trust values that are dependent on the target user, they take into account the very personal and subjective views of the users, they predict different values of trust for every single user based on their own experience. Global trust metrics, on the other hand, predict a global reputation value for each node, based rather on the experience of all other users or on the topology of the social network.

While much work has focused on tools for understanding and adjusting existing privacy settings, Protect_U gandouz_protect_2012 uses machine learning techniques to recommend privacy settings based on a user's personal data and trustworthy friends. Protect_U analyzes user profile contents and ranks them according to four risk levels: Low Risk, Medium Risk, Risky and Critical. The system then suggests personalized recommendations to allow users making their accounts safer. In order to achieve this, it draws upon two protection models: local and community-based. The first model uses the user's personal data in order to suggest recommendations, The second model seeks the user's trustworthy friends to encourage them to help improve the safety of their counter part's account.

Despite the mole of work on social trust, Social Market frey_social_2011 is the first system to propose the use of trust relationships to build a decentralized interest-based marketplace. Similarly, TAPE yongbozeng_study_2015 is the first attempt to combine explicit and implicit social networks into a single gossip protocol. Zeng et al. yongbozeng_study_2015 approaches the privacy quantification problem from a different angle. First, they consider how likely a friend reveals others' personal information, by computing the privacy trust score, which is a widely studied research problem gundecha_exploiting_2011 Furthermore, the proposed work is related to information diffusion in OSNs such as fang_privacy_2010 TAPE framework differs from other work, in considering information diffusion in the context of privacy protection, which requires different sets of features and considerations.

Zeng and Xing zeng_trustaware_2014 studied how individual users can expand their social networks by making trustful friends who will not leak their private information to unknown parties. This work proposes a security risk estimation framework of social networking privacy to calculate the probability of individual privacy leakage through the social graph. The framework is composed of two parts, the calculation of Individual Privacy Leakage Probability (IPLP) and the Relationship Privacy Leakage Probability (RPLP). Relationship Privacy Leakage Probability considers the factors of relationship strength and interactive behaviors. Two vectors namely privacy protection awareness (PPA) and privacy protection trust (PPT) are proposed in this paper to estimate IPLP.

Ostra mislove_ostra_2008 utilizes trust relationship to thwart unwanted communication, where the number of a user's trust relationships is used to limit the number of unwanted communications he can produce. Ostra utilizes the existing trust relationship among users to charge the senders of unwanted messages and thus block spam. It relies on existing trust networks to connect senders and receivers via chains of a pair-wise trust relationship, they use a pair-wise link-based credit scheme to impose a cost on the originator of the unwanted communication. Unfortunately, the scalability of this system stays uncertain as it employs a per-link credit scheme.

Gundecha et al. gundecha_exploiting_2011 propose a

feasible approach to the problem of identifying a user's vulnerable friends on a social networking site. Vulnerability is somewhat contagious in this context. Their work differs from existing work addressing social networking privacy by introducing a vulnerability-centered approach to a user security on a social networking site. On most social networking sites, privacy-related efforts have been concentrated on protecting individual attributes only. However, users are often vulnerable through community attributes. Unfriending vulnerable friends can help protect users against the security risks.

Hameed hameed_lens_2011 proposed LENS, which extends the friend of friend network by adding trusted users from outside of the FoF networks to mitigate spam beyond social circles. Only emails to a recipient that have been vouched by the trusted nodes can be sent into the network. The authors proposed using social networks and trust and reputation systems to combat spam. In contrast, LENS can reject unwanted email traffic during the SMTP time.

SocialEmail tran_social_2010 considers trust as an integral part of networking rather than working alongside an existing communication system. SocialEmail leverages social network trust paths to rate the messages. The key feature of SocialEmail is that instead of directly connecting the sender and the recipient, messages are routed through existing friendship links. This gives each email recipient control over who can message him/her, In contrast, such social interaction-based methods are not sufficiently effective in dealing with legitimate emails from senders outside of the social network of the receiver.

Social interactions (e.g., the exchange of messages between users) have been suggested as an indicator of interpersonal tie strength xiang_modeling_2010 As a consequence, an unsupervised model has been developed to estimate the relationship strength from the interaction activity and the user similarity in the OSN xiang_modeling_2010 Although interaction-based methods leverage social relationships for extracting trust, the applications are not designed to be automated in the sense that the user must explicitly score other users, score messages, create whitelists or adjust the credits.

Vidyalakshmi et al. b.s._privacy_2015 proposed a privacy control framework for information dispersal on social network, they use the quadratic form of bezier curve to arrive at privacy scores for friends, they use the communication information for pre-sorting of friends which is lacking in vidyalakshmi_privacy_2015 Similarly, Akcora et al. akcora_risks_2012 develop a graph-based approach and a risk model to learn risk labels of strangers, the intuition of such an approach is that risky strangers are more likely to violate privacy constraints.

Privacy Index (PIDX) proposed in nepali_sonet_2013 is a measure of a user's privacy exposure in a social network. PIDX is a numerical value between 0 and 100 with a high value indicating high privacy risk in social networks. An attribute's privacy impact factor is a ratio of its privacy impact to full privacy disclosure. Thus, an attribute's privacy impact has a value between 0 and 1. They consider the privacy impact factor for full privacy disclosure is 1.

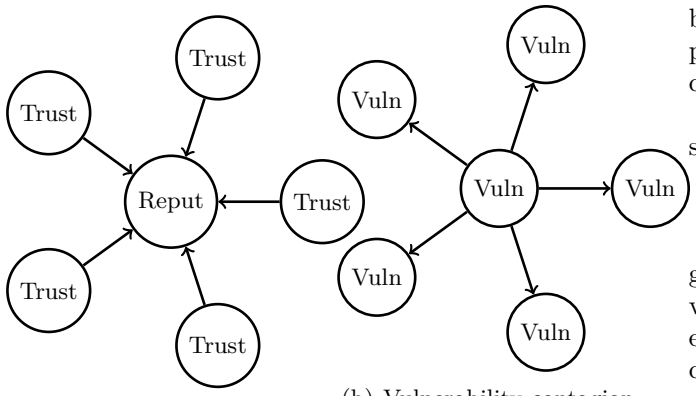
Fang and Le Fevre fang_privacy_2010 proposed a Privacy Wizard to help users grant privileges to their friends. the goal of this tool is to automatically configure a user's privacy settings with minimal effort and interaction from the user. The wizard asks users to first assign privacy labels to selected friends, and then uses this as input to construct a classifier which classifies friends based on their profiles and automatically assign privacy labels to the unlabeled friends. In a similar way, some studies maximilien_privacyasaservice_2009 propose a methodology for quantifying the risk posed by a user's privacy settings. A risk score reveals to the user how far her privacy settings are from those of other users. It provides feedback regarding the state of her existing settings. However, it does not help the user refine her settings in order to achieve a more acceptable configuration.

Abdul-Rahman and Hailes The trust model presented by Abdul-Rahman and Hailes abdul-rahman_supporting_2000 is focused on virtual communities related to e-commerce and artificial autonomous agents. The model defines direct trust and recommender trust. Direct trust is the trust of an entity in another one based on direct experience. Whereas recommender trust is the trust of an entity in the ability to provide good recommendations. Trust can only have discrete labeled values, namely Very Trustworthy, Trustworthy, Untrustworthy, and, Very Untrustworthy for direct trust, and Very good, good, bad and, very bad for recommender trust. The difference between the two ratings from different entities can be computed as semantic distance. This semantic distance can be used to adjust further recommendations. The combination of ratings is done as a weighted sum, where the weights depend on the recommender trust.

All previous work didn't take into consideration the topological aspect of interactions to measure social vulnerabilities of users. The closest study to our approach is that presented in zeng_trustaware_2014 However, this solution doesn't study the social interaction environment of users and the potential information leakage through a vulnerable social environment. In this paper, we study the impact of trusting vulnerable users in preserving the privacy of all users in the communication network.

IV. Approach

The aim of this study is to understand how trust coefficient affects social privacy vulnerability. In this section, we present our vulnerability contagion process in messaging services in order to get social vulnerability scores of users. These scores represent the vulnerability within the social environment of each user. In our study, we focus on the



(a) Trust grant. (b) Vulnerability contagion process.

Fig. 1: Reputation coefficient.

impact of trust and reputation in spreading out the privacy vulnerability.

To model this process we measure the impact of vulnerable users in protecting friends privacy. For example, let us say that a user is exchanging messages with five friends as shown in Figure 1, the reputation of this user is given as the probability to be trusted by his friends (Figure 1a). The more trustworthy a user is, the more reputed he becomes. However, if a user with a high reputation level has a high vulnerability, he can spread his vulnerability with a high infection coefficient (Figure 1b). As a consequence, the social vulnerability of users is calculated as the level of the contagion degree of each user in the communication network. To get these values, a weighted matrix value M is used as an adjacency matrix normalized by users' degree. Social vulnerability is calculated in a continuous space, this means that we iterate the vulnerability contagion process until the process converges.

The probability of the infection is based on the trust level between users.

To evaluate the impact of trust in this process we add a reputation parameter $p_{reputation}$, this parameter is used to know how likely a user could be trusted by his friends, it is calculated as the probability to get at least one trust grant from them.

$$p_{reputation} = p(X \geq 1) \; = \; 1 \; - \; (1 \; - \; p_{trust})^n \qquad (1)$$

Where,

- X: Number of trust grant from friends, $X \sim B(n, p)$.
- n = number of user's friends.
- $p_{trust} = p(X = 1)$: Probability to get one trust grant from a friend.

Trust parameter, in this equation, is added as a coefficient parameter to increase or decrease the vulnerability contagion process. Whether a user can infect other users social vulnerability scores depends on the trust level between them, so users should distrust vulnerable users to preserve their own privacy and the privacy of the entire communication network.

The number of friends infected by each user u in each step of the vulnerability contagion process is given as:

$$new\ infected = old\ infected + p_{reputation} * degree(u)$$

Initial privacy vulnerability scores of each user are given as input to our algorithm to estimate social privacy vulnerability scores, a normal distribution is used to generate initial privacy vulnerability scores. The vulnerability contagion equation is given as:

$$P_{i+1} = p_{reputation} * (M * P_i) + (1 \; - \; p_{reputation}) * P_i \quad (2)$$

Where,

- P_0 is the initial individual privacy vulnerability scores of each user.
- M is the adjacency matrix normalized by users' degree.
- i is the diffusion process iteration level.

The first part of this equation computes the vulnerability of a user based on his friends' average vulnerabilities weighted by the trust level with them. The second part computes the vulnerability of a user based only on his own vulnerability weighted by his friends' distrust level. Social vulnerability is a function of friends vulnerability and the trust coefficient. Mean distances between privacy vulnerability scores of each iteration is calculated to get the convergence process.

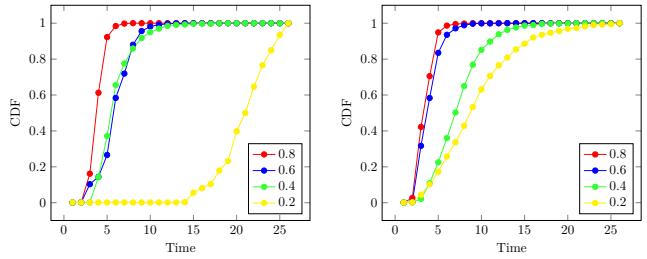
V. Experimentation

To evaluate our contagion process, we used Enron dataset in our experimentation. There are many reasons for using Enron dataset to evaluate our vulnerability measure techniques. First of all, it is probably the only actual corporate messaging service dataset available to the public. Second, it contains all kind of emails "personal and official", so email logs can reveal the level of trust between users by studying the information flow in the network. Finally, this dataset is similar to the kind of data collected for fraud detection or counter-terrorism, hence, it is a perfect test bed for testing the effectiveness of new vulnerability measure techniques.

The properties of the Enron dataset used for our experimentation are presented in table I.

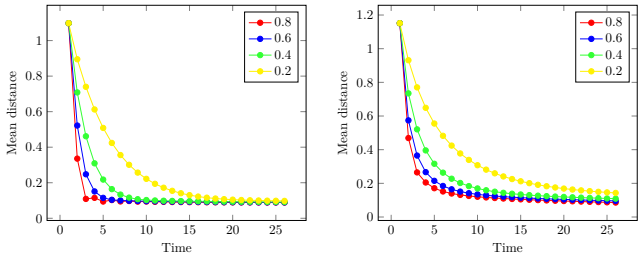
Parameter	Enron dataset	Caliopen dataset
Nodes	958	5885
Edges	6966	26547
Diameter	958	2096
Mean degree	2.413361	9.02192
Edge density	0.00252	0.001533
Modularity	0.654600	0.86526
Mean distance	3.042114	3.914097

TABLE I: Datasets properties.



(a) Enron dataset. (b) Caliopen dataset.

Fig. 2: Cumulative distribution function of infected users.



(a) Enron dataset. (b) Caliopen dataset.

Fig. 3: Diffusion process convergence.

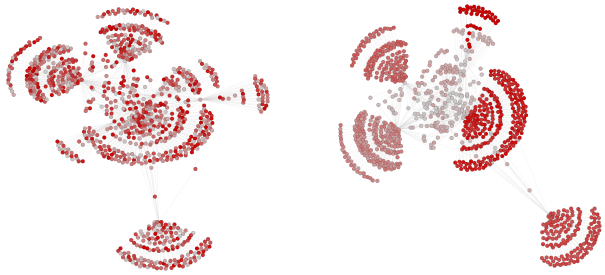
Due to visibility issues, we extract only important nodes given in shetty_discovering_2005 Our substantive interest in this experimentation is in how vulnerability moves through the network. The inputs of our experimentation consist of a set of individual vulnerabilities of users in the network. This set is generated randomly and is represented in the graph of Figure 4a, values of this set are between 0 and 1 and represent the extent to which users are exposed to different kind of attacks such as (phishing, spam, etc). Unlike social vulnerability values, these values didn't take into account the vulnerability contagion process between users. To evaluate how trust coefficient affects our outputs i.e., social privacy vulnerabilities, we variate the trust coefficient through 4 symmetric values 0.2, 0.4, 0.6 and 0.8.

VI. Results exploitation

Below we report the results of applying the contagion process model to the Enron Email dataset.

Figure 2 shows the cumulative distribution function of the vulnerability contagion process, it appears clearly that the vulnerability diffusion process increases as the reputation level of vulnerable users increases, because when the vulnerability contagion process is at its 7^{th} iteration, the cumulative distribution function with the highest user's reputation level (0.8) is 1, this means that after the 7^{th} iteration, all users are infected. This is not the case of users with low reputation level which need further contagion steps to diffuse their vulnerability widely in the network. As a consequence, we can say that vulnerability contagion process speed is highly correlated with users reputation, it infects a large number of users quickly when the user's reputation level tends to 1.

Figure 3 shows the convergence of the vulnerability contagion process, the mean distance between users' social vulnerability scores in each iteration is calculated to see the convergence of the process. The convergence process shows a high convergence level when the reputation coefficient is 0.8. This happens when the mean distance between the users' social vulnerability scores calculated at each iteration still the same. In other words, there are no more users to affect and the contagion process is at its high level. After viewing these tow graphs, we can



(a) Individual privacy vulnerability. (b) Social privacy vulnerability.

Fig. 4: Individual & Social privacy vulnerabilities.

conclude that over-trusting vulnerable users allow them to get a high reputation level and consequently infects the entire social vulnerability scores.

The initial and final measures of the simulation are represented in Figures 4. Figure 4a shows the initial privacy scores, these scores are generated randomly to illustrate the user's individual privacy vulnerability without caring about their friends' vulnerability. Figure 4b shows the final social privacy scores of the contagion process, these scores reveal the social vulnerability of users. Users with dark color are more vulnerable than others with light color in terms of friendship with other users. As a consequence, they have a high level of social vulnerability scores.

User ID	Individual vulnerability	Social vulnerability
34	0.84	0.67
67	0.12	0.87
206	0.76	0.33
588	0.23	0.78

TABLE II: Difference between Individual & Social privacy vulnerabilities.

Table II illustrates the input (Individual vulnerability) and the output (Social vulnerability) values of four arbitrary users of our dataset. Results show that users with low individual vulnerability (e.g. user 67) could have a high social vulnerability due to their interactions with vulnerable users. In contrast, users with high individual vulnerability (e.g. user 206) can, in turn, be less vulnerable

from interactions with other users, but harms considerably the social vulnerability of their interlocutors.

In summary, results presented in this section show that if the trust coefficient between users is up to 0.8, the vulnerability diffusion process through trust relationship is at its high level of speed. This what happens when a new information appears in a communication network and users forward it largely in the network. In addition, this work gives a new insight to understand the relationship between trust, reputation, individual vulnerability and social vulnerability in the context of messaging services such as emails.

VII. Conclusions

This paper studies the relationship between trust and reputation metrics in users' interactions and the social privacy vulnerability of users. We observe that such metrics, severely affect users' privacy in regard to their social relationships. Trust coefficient in the social network graph plays an essential role in spreading vulnerability. Our experiment investigates the probability of infecting other's privacy by increasing the reputation of vulnerable users. In this case, the number of nodes infected depends on the trust grant assigned to vulnerable users. Our experiment reveals also that the social vulnerability of users could be extracted from their individual vulnerability by applying our vulnerability contagion process. Privacy-preserving in online social network architectures should address this problem by discouraging trusting vulnerable friends.