International Journal of Business and Social Research
Issue 11, Volume 04, 2014

Social Web Identity Established upon Trust and Reputations

Rajni Goel[1]

ABSTRACT

Online social networks have become a seamless and critical online communication platform for personal interactions. They are a powerful tool that businesses are using to expand among domestic markets. The increase in participation in online social networking can and has caused damage to individuals and organizations, and the issuance of trust has become a concern on the social web. The factors determining the reputation of persons (customers) in the real world may relate to the factors of reputation on the social web, though relative to how trust is established in the physical world, establishing trust on the social web can be fairly difficult. Determining how to trust another individual's online social profile becomes critical in initiating any interaction on the social web. Rather than focusing on content on the social network page, this research proposes and examines the application of user reputations to determine whether the trust should be issued on the social web. A top-level framework to establish trust in an identity on the Social Network Sites (SNS) as a function of the users' associations, usage patterns and reputation on the social web is presented.

Keywords: Identity, reputation, social networks, trust.
JEL Codes: L82, M31.
Available Online: 22nd November, 2014.
MIR Centre for Socio-Economic Research, USA.

1.0 INTRODUCTION

Social networking has become a force multiplier in the way individuals and organizations communicate and interact on a personal and professional level. Over the past decade social networking, open publishing in general, connections through individuals have rapidly became a popular tool that businesses are using to expand. Some of the known and most popular social web networks include Twitter, Facebook, MySpace,

[1] Associate professor and Chair, Information Systems and Decision Sciences, Howard University, United States, E-mail: rgoel@howard.edu

Meetup, LinkedIn and Google+. As the number of available social web networks rise, subcategories have been developed to group the services which they provide. The subcategories include: business, common interests, dating, face-to-face facilitations, friends, pets, and photos (Gross, & Acquits, 2005). Though these different types of social web networks provide different user functionality, where they overlap is in their core feature which offers user profiles that serve as a digital representation of users, to others in order to pursue with the intention of contacting or being contacted. In user profiles, personal information as name, date of birth, thoughts, photos and so much more is displayed for the public to see. All of this information is aggregated to form digital identities which then develop reputations among other social web users. In face-to-face interactions, individuals accomplish authentication of another simply through identification, but this ease of authentication is not found in the social web. This has raised concerns regarding user trust and reputation on the social web, concerns that will continue to shape the use and interactions that take place on the social web. Recently, companies initiated processes to review social networking connection data to determine business risks; instead of relying primarily on credit scores as FICO (review payment history), financial lending companies use social connections as an indicator of person's creditworthiness (Singh & Bawa, 2007).When in person, the reputation and validity are evaluated to determine if a person could be trusted; entities maintain a set of reputations for individuals whom they know. When we need to establish a connection with a new (unknown) entity, we ask people with whom we already have relationships for information about that new person. Similarly, we believe a trust in an identity on the Social Network Sites (SNS) is a function of your associations, usage and reputation on the social web. This notion is better understood by first investigating the following hypothesis: Social web users should issue trust based off of the digital identity representations of their usage patterns and interactions with other social web users.

The measuring of user behavior on the online social web has been receiving attention recently by researchers. Some have created a measurement framework to observe user activity and provide comprehensive measurement analysis of total usage and behavior as examined on popular Online Social Networks (ONS) and further classify users into groups based on their usage patterns (Gyarmati & Trinh, 2010). Others have provided timing information of active users based on packet level traces (Benevenuto, 2009). But little work has been done in relating online usage behavior to the attribution of trust and reputation on OSNs. Most of the work in trust and privacy on the social web has been focused around developing trust inference algorithms. At times, inferring trust using a mathematical algorithm can be less than accurate due to the fact that they do not account for the varying circumstances along with the human interaction which is unpredictable. The decision on whether or not a user should issue trust should be based on the authentication and credentials of a user that is developed and found within the social web identity and reputation of users. We propose to use the usage data to establish a social identity value as reputation measure that is based on a user's collective connections and engagement on the social web. This model would include attributes as the number of connections, types on connections, number of visits, along with others. The goal is to assist in the decision making process as to when or when not to connect with an online social network user; this reputation value based on trust of identity would provide a data point to assist in the process. A well-developed trust architecture based upon a strong trust model is the key to establishing trust for a social network user.

This paper proceeds as follows. First, the background on trust, identities, and reputation in the social web environment is discussed. Next, the notion on how identities and reputations are formed and used to establish trust among individuals in the real world is presented. Then, a novel framework to determine an individuals' Social Identity (SID) value using their usage patterns on the social web is created and related to using it to authenticate a user to forma trust. Finally some conclusions and future directions for work are stated.

2.0 RELATED WORKS

Work has been done on what defines a user, of the social web, in relation to their identity, and how social web and real-world identities differ. In (Rowe, 2010) a user study was conducted to analyze the difference that may be found in the user's digital social network and real world social network. Patterns and behavior were reviewed to help come to the conclusion that of those who participated in the study, have digital social networks that mimics their real world social networks. To think about a digital social network that aligns to a real world social network, you may wonder what information is being provided for users to authenticate and trust each other for networks to be formed. At Carnegie Mellon University a research study was conducted amongst 4000 students and discussed in (Gross, & Acquisti, 2005). The common pieces of information that users place on the social web profiles were established. Examples from this study about personal information posted include: 90.8 percent of users upload images, 87.8 percent posted birth dates, over 50 percent shared current addresses and 39.9 percent shared their phone numbers. This study investigates the types of personal information and the frequency at which this information is being made public through the social web. These kinds of personal information of users can be analyzed and categorized as asocial web identity to better understand user behaviors.

Moreover, online usage measurements have been used to address issues of online social networks as characterization of user activities and usage patterns in the examined OSNs (Gyarmati & Trinh, 2010). The main findings of (Gyarmati & Trinh, 2010)do not address social identity or reputations, but rather focus on how users' online time spending can be modeled with Weibull distributions. More the authors discuss how during the duration of each SNS visit, a fraction of users tend to lose interest surprisingly fast; and furthermore the duration of OSN users' online sessions shows power law distribution characteristics. These types of results can then be further integrated with other usage behaviors to attribute trust to the user. From a reputation perspective, in (O'Connor &Griffin, 2009) a reputation system was developed that utilizes data mining and inference to generate user reputations, leveraging information in the social web. The goal of this system was to provide means to authenticate user reputation in the social web to help increaser users' trust of digital interactions. Other algorithms have been created to try to emulate and predict trust occurrences such as the one we find in (DuBois, Golbeck, & Srinivasan, 2011) which combines a path-probability trust inference algorithm with a novel technique using spring-embedding to classify the relationship between two users. It is also mentioned here though that "it is not unreasonable to question whether or not trust can be accurately computed at all."

This led to the work found in (Kagal, Finn, & Joshi, 2005) that provides a distributed trust management architecture that involves proving that a user has the ability to access some service or resource by verifying that the user's credentials comply with the security policy in place. This gives a different approach to trust in the social web by not trying to algorithmically calculate trust being issue but allowing users to verify the identity of a user to determine if the trust should be issued. Similar social identification mechanisms have also been proposed to address the issue of trust in (Hogben, 2009) where users are issued tokens that contain a public-private key pair and trust ratings are given to each token as the user interacts with others. But, establishing social web trust ratings relative to social behaviors with other users is lacking being addressed in the current research arena. The notion of the Klout score (Klout, 2014) may seem similar, though the Klout score measures popularity not trustworthiness. In essence, both the technological and social forces (working together) shape the inherent operating constraints in social networks. In the real world, indirect cues, notes and transparencies in ones associations and relationships assists in assigning a reputation/trust index to an individual. Online social web user trust can be modeled similarly. The issue we explore here is how the social web users' behaviors, associations, postings and frequency of interactions can be analyzed and modeled to able to put form their reputation. This emergence and explosive growth of SNS has led to the prevalence of threats due to misused trust and must be controlled. Our conceptual

model maps the method in which we establish trust in identities in the physical world relationships to online networks.

3.0 REPUTATION IN THE REAL WORLD

There is a great deal of work that has been done surrounding trust and privacy in the social web, developing different models and algorithms on how trust is issued and probabilistic inference that trust exist between mutual relationships. (Adali, Goldberg, Hayvanovych, Magdon-Ismail, Szymanski, & Williams, 2010)believes that users issue trust in the social web based on how users establish trust in the real world. In the real world we define trust as the willingness of a party to be vulnerable to the actions of another party. In order to develop this willingness, five factors are evaluated which include identity, communication, past interactions, and associations. Identity is the personal information of a person that includes the name, hometown, date of birth, etc. When it comes to communication, the validity of what a person tells other is evaluated. If someone has past interactions that are less than desirable, the issue of trust will come into question. Another important factor is the examination of individuals with whom a person associates. All of these factors come to form the reputation of a person. In (Rowe, 2010) social web reputation is established based on user *identity*, which is defined with a different definition from that of the real world definition mentioned earlier. Identity, in this case, consists of a three-tiered approached defined as (Rowe, 2010):

1. *My Identity*: Includes information that is persistently constant such as name, age, date of birth, etc.
2. *Shared Identity*: contains information that will change over time, as a person adds and removes friends from their user profile.
3. *Abstracted Identity*: consists of information that is gathered through groupings and demographics formed over time as the user changes their preferences.

4.0 FRAMEWORK FOR SOCIAL WEB REPUTATIONS

In the real world authentication of the factors that create reputation, is completed through separate entities such as identification cards. Whereas on the social web, the same form of authentication is not available. Our framework to develop a social identity reputation score is based on effectiveness of measuring collective human behavior; analyzing the recurring and quantifiable principles of human social interactions as represented in digital form. The underlying premise is the inability to know what any one particular individual or social connection signifies; but, collectively measuring variations the friendships, frequencies, longevity of stay on line, opinions, and personal information provide varying degrees of reliability.

We can see where the overlap occurs with the factors of trust in the real world. As identities are developed we find that reputations are built for users, partially based on their connections. In (O'Connor & Griffin, 2009), it is stated that reputations form an important part of how trust is granted amongst individuals. In the physical world, more social interactions among two persons predict to a stronger connection (trust) between them. Trust in the context of social networks is a complex process because it requires all participants to disclose a lot of information about them; hence we focus on basing the trust on a reputation social identity which is constructed using frequently logged data, rather than personal posted information.

Trust is widely accepted as a major component of human social relationships. In general, trust is a measure of confidence that an entity will behave in an expected manner, despite the lack of ability to monitor or control the environment in which it operates (Singh & Bawa, 2007). In (Kramer, S., Gore, R., & Okamoto,

2010), the authors noted that there are three distinct aspects that determine the concept of trust in the system:

1. Trust relations: The interaction between two entities in which they believe or know that the other entity is operating in an honest manner.
2. Trust domains: A community of mutually trusting entities in which there are a universal belief and a sharing of knowledge takes place among all entities within the community.
3. Trust management: The organization of trust relations into trust domains and ensures the flow of trust negotiation between all participating entities.

From these three distinct aspects, we deduce that trust is very much based on the establishment of building a reputation amongst all participating entities. Trust relations can be further broken down to incorporate potential metrics identifying each entity, and these metrics can then be compared to a minimum trusted threshold. We propose that one way by which individual's level of reputation can be formed is by measuring usage and linkages of each social entity. Measurements to calculate a *Social Identity (SID)* value would include the following:

1. Number of social networking groups an individual belongs to (on the average).
2. Probability that an individual accepts or rejects an invitation to join a group, or the individual accepts and rejects someone asking to join his/her group.
3. Number of relationships an individual maintains at a given time (on the average)
4. Amount of individual traffic volumes and then compare to the others on the social networking site.
5. Individual size or membership compared to the other social networking sites
6. Individual usage statistics – and then compare them to other social networking sites
7. Individual target social groups are broken down by age, gender, race, education, religion, etc.

We can summarize above data from which SID value can be calculated in Table 1:

Table 1: SID value

1. Social Reach	Number of relationships an individual maintains at a given time (on the average), number of different Social network sites' membership, Individual target social groups broken down by age, gender, race, education, religion, etc.
2. Identity Usage	Individual usage statistics – length of stay, time of day, amount of individual traffic volumes, number of social networking of which you are member; Probability that an individual accepts or rejects an invitation to join a group, or the individual accepts and rejects someone asking to join his/her group.

The *SID value* will be calculated based on user usage characteristics and social behaviors to determine a predictive model for a social reputation and trust. Our continuing research involves gathering the data to determine thresholds of determining the *SID value* and connections which assist in establishing thresholds of trust. For example, the SID value if determine if users who are more selective about connecting on a social network, may lead to fewer friends on average, resulting in stronger trust relationship among them.

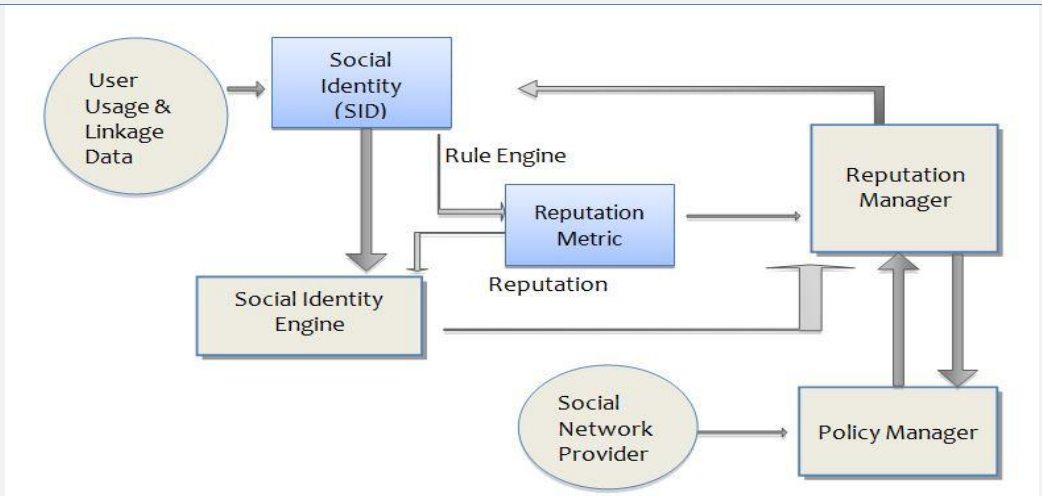
To check the validity of a user's reputation(O'Connor & Griffin, 2009), created a system that provides independent validation by generating "combined digital identities found on different social web networks, using publicly-available information sources to find both different parts of one identity, and the links between different identities."Our framework, however, will be a top-level explanation of the components and management of the social identity measure (Figure 1).This establishes a level of reputation.

Components of the framework include:

1. Reputation Manager - The Reputation Manager will collect and manage the reputation metrics, which are based on the logs of the values to the questions stated above.

2. Policy Manager - The policy manager manages the security policy established by the social network provider. Additionally, the policy manager manages each user's identity usage information. The policy manager uses the data collected by the Reputation Manager.
3. Social Identity Engine -The Social Identity Engine compares the reputation metric against minimum reputation metric that determines if the reputation should be considered as weak or strong.

Figure 1: Framework



The minimum reputation metric is a value determined by using prior work and techniques stated by prior established researchers as (O'Connor & Griffin, 2009).A wealth of research in the area of sociology and real world interactions will be used to initialize these engines. Utilizing the human social networks properties and models will provide an insight and potential generation of policies and rules for the Web-based social networks. This will then assist in attribution of reputation and trust online.

5.0 CONCLUSION & FUTURE WORK

In summary, this paper introduces a unique approach to establishing an online social network user's digital reputation and trust based on usage instead of the content posted on the OSN sites. The factors that define reputation in the real world are the same of those that are used to define reputation on the social web, yet managing these reputations within an information system is the challenge that is investigated. Just as the reputation of an individual is used to establish trust of that entity in the real world, the same can be done on the social web. The proposed frame work establishes a *Social Identity* (SID) value based on a user's usage and associations' data is proposed. The SID value is used by the reputation manager to assign a level of trust. Due to this need some researchers are developing systems that will be able to crawl numerous social web networks to verify the validity of information that forms a user's reputation. With the use of systems such as the one presented, social web users will be able to determine if the trust should be issued.

Online social network provider's policies will be influenced by the reputations of customers using their applications. Future work concerning reputations of users on the social web should include further formalizing a more robust framework and quantitative model and experimentation by collecting data (or using existing repositories) to determine *SID values* and creating reputation metrics. Also, a comprehensive list of social network provider's policies and the level of breaches to policies must be collected and synthesized in order to model the reputation thresholds. Lastly, more adaptive learning and the adjusting

model of the reputations by the engines may be necessary, as well as automated recommendations to OSN provider's policy adjustments. This will lead to the online social trust environment as we experience in the physical world.

ACKNOWLEDGEMENTS

Special Thanksto Sharnay Clark, a Computer Science student who graduated from Howard University for her assistance in initiating and developed the research for this work.

REFERENCES

Adali S., Escriva R., Goldberg M., Hayvanovych M., Magdon-Ismail M., Szymanski B. W. W. A., Williams G.(2010).Measuring Behavioral Trust in Social Networks. Intelligence and Security Informatics (ISI), *IEEE Int. Conf*., Vancouver, BC, 23–26 May 2010.

Benevenuto, F. (2009).Characterizing User Behavior in Online Social Networks.Proc. ACM SIGCOMM Internet Measurement Conference.

DuBois, T., Golbeck, J., Srinivasan, A. (2011).*Predicting Trust and Distrust in Social Networks*.Univ. of Maryland, College Park, MD USA.

Gross, R., and Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks. Proceedings ACM Workshop Privacy in the Electronic Soc. (WPES'05), ACM press, 71-80.

Gyarmati, L., Trinh, T. (2010).Measuring User Behavior in Online Social Networks. *IEEE Network*, 24 (5), 26-31.

Hogben, G. (2009). Security Issues in the Future of Social Networking. *ENISA Position Paper for the W3C Workshop on the Future of Social Networking*, BC, 15-16.

Kagal, L., Finn, T., Joshi, A. (2005). *Developing Secure Agent Systems Using Delegation Based Trust Management*, University of Maryland Baltimore County, MD USA.

Klout (2014).Retrieved on September 29th 2014 from https://klout.com/home.

Kramer, S., Gore, R., & Okamoto, E. (2010).Formal definitions and complexity results for trust relations and trust domains. Retrieved March 10, 2012, from http://www1.spms.ntu.edu.

O'Connor, B., Griffin, J. (2009). Mnikr: Reputation Construction through Human Trading of Distributed Social Identities.

Passant, A., Kärger, P., Hausenblas, M., Olmedilla, D., Polleres, A., Decker, S (2009).Enabling Trust and Privacy on the Social Web.*W3C Workshop on the Future of Social Networking*.

Rowe, M.(2010). The Credibility of Digital Identity Information on the Social Web: A User Study. WICOW' 10.

Sherman, E. (2012). CBS News. Retrieved April 22, 2012, from CBS News: www.cbsnews.com.

Singh, S.,Bawa, S. (2007).Privacy, trust and policy based authorization framework for services in distributed environments. *International Journal of Computing Science*, 2 (2), 85–92.