MeT: *Personal Transaction Protocol Version 1.0*, Draft Specification 01-11-2002, Mobile Electronic Transactions Ltd., 2002.

Mozilla Project: *Privacy and Security Preferences*, PSM 2.0 Help *http://www.mozilla.org/projects/security/pki/psm/help_20/passwords_help.html*

NIST: *Electronic Authentication Guideline*. Nist Special Publication SP 800-63, June 2004.

NOIE: *Australian Business Number Digital Signature Certificate (ABN–DSC), Broad Specification*. National Office for the Information Economy, September 2003.

OASIS: *Security and Privacy Considerations for the Oasis Security Assertion Markup Language (SAML) V2.0*. Oasis Committee Draft 01, 18 August 2004.

USOMB: *E-Authentication Guidance for Federal Agencies*. Memorandum M-04-04 to the heads of all departments and agencies, US Office of Management and Budget, 16 December 2003.

Wong R, Berson, T and Feiertag, R (1985): *Polonius: An identity authentication system*, Proceedings of the 1985 IEEE Symposium on Security and Privacy, pages 101-107, 1985. *http://www.anagram.com/berson/abspolo.html*

7

Trust Models for Community-Aware Identity Management

Hee-Chul Choi, Sebastian Ryszard Kruk, Slawomir Grzonkowski, Katarzyna Stankiewicz, Brian Davis and John G Breslin

The contemporary Web is heading towards its next stage of evolution. From a clump of unorganised information spaces, the Web is becoming more focused on the meaning of information (the Semantic Web) and on community awareness (Web 2.0). One of the key concepts in this new Web is that of social networking, where both sophisticated trust modelling and personal identity/reputation management are required for the creation of social networks and for the exchange of information in these networks. The Web has many instances of sites and services where reputation management and trust form the basis of social and commercial interaction between members of those sites. However, there are few systems that enable users to share their credentials among many websites. It is also important that systems should provide strong security and protect user identities, but all of these features should also be transparent from a user's perspective.

In this article, we begin by detailing how trust can be modelled within online communities. We present methods for constructing community-aware identity management systems and for computing trust levels between users of a social network, using a novel trust model that takes advantage of both the capabilities of the Semantic Web and of a distributed topology. We also describe how the trust of a particular person relies on the separate social networks that they are members of. Finally, we evaluate our research against current studies in the psychology domain.

1. Introduction

The contemporary Web is heading towards its next stage of evolution. From a clump of unorganised information spaces, the Web is becoming more focused on the meaning of information (the Semantic Web) and on community awareness (Web 2.0). One of the key concepts in this new Web is that of social networking, and sophisticated trust modelling is required for the creation of social networks and for the exchange of information in these networks. Online communities, blogs, wikis and other Web 2.0 technologies are strongly related to social networks, and also require trust algorithms. Online social networks should resemble real world social networks, and therefore research on identity management and trust modeling must deliver proper models and algorithms corresponding to real world examples.

The Web has many instances of sites and services where reputation management and trust form the basis of social and commercial interaction between members of those sites. These range from social networks for creating business contacts and employment opportunities, to voluntary community groups working towards a common civic goal or the development of an open source software project, to forums or dedicated auction sites for buying and selling goods on-line. For those that are operating as commercial entities, sites that allow online payments and offer services in several countries or states are often complex systems that require sophisticated reputation management measures.

Existing approaches like e-Bay (1) offer only simple solutions. One is able to check the amount of positive or negative opinions a user has, but one cannot check if the person from whom we are going to buy an item was recommended by our friend or by a good friend of a friend. However, the opinions of people we know and trust should be thoroughly considered. Then if we consider undertaking a serious transaction, we could also take into account the overall virtual reputation which usually gives us a first impression.

The ideal solution for such a problem should take advantage of an advanced social network system that would be close to a real world model (especially since these sites often involve real world transactions). Additionally, the system must be easy to use and will enable users to share credentials among many websites. What is most important is that a system should provide strong security and protect the user's identity, but all of these features should also be transparent from the user perspective.

FOAFRealm (12), an identity management system, seems to satisfy the aforementioned requirements. The proposed social network model extends the popular "Friend Of A Friend" (FOAF) user profile standard (see section 2.2.2). Using FOAFRealm, stored digital identities can be shared among the various services without loss of reliability or confidence. Also, various security features are required by such a system, and their implementations are explored in (24).

While developing new systems, we have to remember that the role of computer science is reduced when the system is delivered in a ready-to-use state to the end-user community and its adoption becomes widespread. It is at this stage that the role of psychology begins, as both lay people and code "hackers" begin to interact within the developed virtual world. This is important because an ideal model of trust must also consider the various aspects of human behaviour in such a virtual world and provide solutions that are independent of the user's experience. We will show how our work tries to combine both the novel technological achievements of FOAFRealm (28) and psychological science (see section 5).

1.1. Related Work

The meaning of trust in this article is based on many different aspects of computer science, psychology and sociology and we will briefly describe some of them below. The first domain of interest is that of trusted systems, which are mainly

related to security engineering. This domain encompasses areas such as risk management, surveillance, auditing and communications. Extensive knowledge on security engineering has already been collected and analysed by Taipale (35) and has been researched in the Trusted Systems (2) project, which is a part of Global Information Society Project (3) lead by the World Policy Institute (4). It investigates systems in which some conditional prediction about the behaviour of people or objects within a system has been determined prior to authorising access to system resources.

Secondly, there is the concept of "web of trust" systems. This concept is related to cryptography and focuses on technologies like PGP (5) (see section 2.2.2), Open PGP-compatible (6) or public key infrastructure (PKI) (7). They offer solutions, which require the trust endorsement of the PKI generated certificate authority (CA)-signed certificates. The last and most popular concept is called a trust metric. It is also considered within the areas of psychology and sociology. The aim of it is to propose a measure of how a member of a group is trusted by other members. A comprehensive overview of such metrics has been prepared on the Internet community at (8); it presents a brief classification and provides many examples.

Existing metrics are diverse in many aspects. TrustMail (23) and FilmTrust (22) propose to take advantage of a Semantic Web-based social network, whereas other ideas also based on graph walking use a far different approach like subjective logic (25).

Furthermore, an interesting model was proposed in the PeerTrust Project (9, 34), which concerns a decentralised Peer-to-Peer electronic community. The important contribution of these authors is to build a trust model that considers only three factors: the amount of satisfaction established during peer interaction, the number of iterations between peers and a balance factor for trust.

The EigenTrust (26) algorithm has similar ideas to PageRank (31) but has been used in the context of file-sharing systems. This method computes global trust for peers, where the value is based on the history of uploads. It enables the system to choose the peers with a history of reliable downloads. Therefore, malicious peers can be excluded from the network.

Although much of the previous related work presented in this article is related to trust metrics, our approach differs from this work with regard to several fundamental aspects. We propose a novel trust model that takes advantage of both the capabilities of the Semantic Web and of a distributed topology.

1.2. Outline of This Paper

The remainder of the paper is organised as follows: section 2 describes community-aware identity management, section 3 details models of trust, section 4 discusses social network management and section 5 describes our evaluation phase. Finally, section 6 presents conclusions and future work.

2. Community-Aware Identity Management

In this section, we describe the concept of identity with respect to an online community and also the importance of trust and the social network. Moreover, we describe ways to capture trust within the online community.

2.1. Community Aware Identity

Online communities are currently overflowing with identities. It is not difficult to utilise multiple identities on the Web. We can easily obtain a new identity on the Web such as a portal ID, an email address or an identity for a new blog. This can create the following problems, making it difficult to trust information within an online community:

- A person has the opportunity to behave irresponsibly online;
- A person can misuse his/her identity to send spam or distribute obscenities;
- A person is open to acting more aggressively online, "flaming" other users and "trolling"; and
- A person can distribute information without peer-verification or peer-review, knowingly misinforming others.

There are some methods, however, to prevent the issue of identity corruption. For instance, an invitation is needed if one wishes to become a Gmail[1] or orkut[2] user. However, users can deceive these systems by inviting themselves to create new identities or by making use of automatic invitation spoofers[3]. Some portal

sites[4] require a valid name and corresponding social security number to join. However, despite many usage benefits, these portals can have problems protecting privacy, and preventing the leakage of personal information from smaller portal sites is still an ongoing issue.

The reader may also find CAPTCHAs (33) of interest, which are an elegant way of thwarting automated spamsending systems by requiring an agent to perform a task that only a human could do. For human beings intent on identity corruption however, these systems do not solve the problem.

To solve identity corruption, the concept of trust or reputation is introduced. It can be partially yet successfully applied as an alternative to identity. For instance, e-Bay (1) helps users to find more reliable sellers via their reputation system.

However, the concept of trust has not yet been widely applied throughout online community sites. It is difficult to model since it is defined by number of aspects, it is affected by various factors, and finally it is difficult to quantify.

To clarify identity or trust within the online community, we must consider how identity and trustworthiness are realised within a real-world community. In the real world, the identity of a person is more constrained:

- It is not easy to use multiple identities;
- A number of social relationships are linked with each person.

Jean (16) surveyed some useful operational definitions of trust, and found that trust can be interpreted as 'a willingness to cooperate' and 'a willingness to share personal information'. This demonstrates a close connection between other social relationships and trust. Therefore, trust can affect other relationships, and likewise, trust can be calculated via other social relationships.

2.2. Identifying Trust on the Online Community

We now describe one of the key issues: how can we extract a trust level, i.e., how do we digitise trust as a value? There are two kinds of approach. The first approach is often called a reputation system. In this approach, systems collect user actions or other facts. The facts are calculated and notified to other users as a reputation

level. The second approach is more active: a user can express trust with another user. It is a more subjective and user-centred approach. Therefore, we call the first one a machine-driven approach and the second one a user-driven approach. In this section, we describe these two approaches and present a hybrid approach.

2.2.1. Machine-Driven

Approaches Machine-driven trust systems can collect information with-out any intended user interaction. This approach can be easily adapted within a website or even to the whole Web because it does not require human effort. For example, the PageRank (31) method from Google[5] demonstrates how to calculate the trust of numerous web pages. Furthermore, trust can be evaluated by polyphasic facts:

- It provides values that are more objective than a user-driven approach;
- It is easier to capture trust as a numerically;
- It is easier to rank a person or a page.

The trust of a user can be calculated via the relationship with other users in a similar manner to how the trust of a page can be evaluated via hyperlinks with other pages (as PageRank (31) demonstrates). The relationships among human beings and their patterns are essential to social network analysis (21). If we assume hyperlinks to represent social relationships, social network analysis can be applied and can help to express social identity within the online community.

There are some attempts to obtain trust via indirect facts available within an online community: some bulletin boards provide additional information such as when users registered their accounts and the total number of posts that they wrote[6]. The number of posts and registration date of a user can demonstrate indirect trust related to a user's identity since the user did not change their identity for a period of time and user already has established a number of relationships with other users. Some examples of indirect facts that may allow a user A to gauge the trust of another user B include instances where B replied to threads that A created or replied on, or B posting or subscribing to the same forum as user A. More direct connections are established when A and B both send private messages to each other through the bulletin board system, or when A and B are linked through a "buddy list" system. Some bulletin board systems[7] also amply "karma" reputation systems, that are part user-guided and machine-driven

(users can give positive or negative points to other users, but the system can automatically disable accounts reaching a certain negative threshold).

An interesting machine-driven approach proposed by the authors involves the mining of data from mail servers. A single company can provide mail addresses for all employees. The employees in the company may utilise the same mail server for their work. This mail server could count how many mails a user has received from the same organisation. This value would represent the level of cooperation achieved in the workplace. Therefore, it can be interpreted as a trust value or position/rank of the user within the company. This could be applied to any other kind of intranet messaging system.

As the Semantic Web is populated with more data, it becomes easier for machine-drive approaches to mine trust information. Such information can be mined from Semantic Web data produced by online communities, for example using the FOAF or SIOC[8] ontologies. For example, in blog communities, mutual blogroll links between users imply a certain respect for the content on each other's blogs, and connections can be made between users. Ecademy[9] also creates FOAF knows relationships between users who have sent each other private messages through the site, and this could be augmented with trust information.

However, the machine-driven approach has definite defects. It is usually calculated as an analogy which can provide a false result, therefore the machine-driven approach is difficult to use within critical areas. As it is also machine-centred, a user cannot apply their personal intention and style to the computed trust levels.

2.2.2. User-Driven Approaches

The user-driven approach does not provide as much trust data as the machine-driven approach. However, it does not need to extract trust from indirect data: a user will provide the information directly themselves, a system can be designed in a creative way. It is closer to the user's perspective and easier approach to modelling trust. For this reason, most trust systems try to use a user-driven approach. Below we describe significant user-driven systems and some important facts which must be considered.

PGP. PGP-based systems (36) have made cryptography available to a mass number of users who needed on-line privacy. The project breaks the traditional

hierarchical trust architecture in that it applies an approach without a central authority. The fact that PGP makes use of asymmetric key encryption means that each user must generate their own private and public key pairs. Additionally, a public key can contain a user's ID information, a timestamp, (which will inform the user when was the key was created), and finally the public key. If user A believes that the copy of user B's key is reliable, then user A can sign the copy. Moreover, user A may decide to pass the signed copy to another user – user C. In this way, user A becomes an introducer and the signed key becomes a certificate. PGP requires users to tell which introducers they trust and how much they trust them. Each user stores obtained certificates, so as to enable PGP to calculate a validity score for each public key. To summarise, PGP-based systems establish the authenticity of binding between a public key and a user, and it is unrelated to the trust value between users. The approach proposes a exible way to communicate, because there is no need to exchange a user's key pairs by means of secure channel. Since trust decisions are in the hands of individual users, intelligent observation and caution are required by users. The PGP has one severe drawback: there is no quick and reliable way to propagate information about expired timestamps and comprised keys among users.

FOAFRealm. From the perspective of trust, the FOAF-Realm (28) system combines several novel technologies. The most important is FOAF (10), a semantic profile description standard that makes it feasible to merge and process profile information with computers. The FOAF standard defines a set of fields describing a person. Users can be distinguished between each other via a unique email identifier. Furthermore, they can define relationships amongst themselves. The main drawback is that the relationship information is stored in very simple manner. In FOAF, a user may only know (or not know) who another user is through a "knows" relationship. It is not possible to set any other relationship parameters except "knows". Unfortunately, it is very often necessary to set a knows friendship level such as: "never met", "average" or "very well".

The FOAFRealm system has advanced the standard and applied the aforementioned friendship level field, and thus has moved closer to the real world situation. Since a FOAF relationship can be very long (i.e., many degrees of separation) or since a user may want to restrict the distance between himself and a friend of a friend, a user can also specify the maximum distance value.

Resources can be managed in Access Control Lists (ACLs) by means of a Social Semantic Collaborate Filtering (SSCF) (29) component and each resource can be controlled separately. To sum up, this system allows one to share bookmarks and community documents among the friends one knows and trusts, as well as their trusted friends.

Applying Multiple Relationships. In the real world, a person's trust can have multiple values: a workaholic person can be trusted by colleagues but he or she may well be less trusted by their family (see 3.1). To capture a more realistic social network on the Web, more varying trust relationship models are needed. However, a system designer cannot model every relationship that users require and furthermore cannot construct the perfect questionnaire to capture total information about relationships.

Yubnub[10] introduced the interesting concept of shared user-defined information on a website. Users can define their own commands for themselves: other users also can use these commands. For example, one user can define a command to check weather. A user just needs to provide some arguments and a site URL of a weather report site. Then, another user can use the new 'weather' command to check the weather. Through user participation, Yubnub is evolving by itself without the need for painstaking research and development.

This could be applied to shared relationship information. For example, a user could define a "good father" relationship and give a 90% trust rating for his/her family. Then, another user could find the "good father" in the ordered list of relationships for a family network. Autocompletion can also help to discover the relationship.

Limitation of User-Driven Approaches. There are two obvious limitations to the user-driven approach. Firstly, a user must describe the information. Without the significant benefits of user encoding, it is hard to collect basic information for computation. Examples such as Yubnub and del.icio.us[11] overcome this difficulty by orchestrating the needs of the user and the required information. Therefore, designing a user-driven system should be based on user requirements. Secondly, it is limited by the distance of relationship: for a user, it is hard to capture the general reputation of a stranger if the profile or actions of a user can be blocked in a partially restricted view of a community.

2.2.3. Hybrid Approach

We have introduced two approaches, including their advantages and disadvantages. We found that the machine-driven and user-driven approach complement each other: The machine-driven approach can be overcome by human input; the network disadvantages of a user-driven approach can be fixed via a reputation system. Therefore, we move to present hybrid approach that integrates both advantages.

A hybrid approach should be based on a user-driven approach: a machine-driven approach cannot provide the trust value itself, it is impossible to model the total information relating to trust since one cannot read the mind of a user. Therefore, one should utilise a user-driven approach in order to model human trust.

However, a hybrid approach should of course be supported by machine-driven approach. A machine-driven approach can provide the trust value of an unknown person. Through a machine-driven approach, one can model the real-world concept of reputation; one therefore has the opportunity to make new connections in an unexplored online world. Therefore, one can take advantage of the online community and create a new identity management system for that online community.

3. Trustmodels and Computations

Proper modeling of social network interactions and computational algorithms is crucial for identity management systems based within an online networking paradigm. Moving forward from the old model of identifying users based on login-password-group(s) triples to the trust delegation model recently introduced poses, amongst others, the question of how to model and compute the trust and relationships so that they reflect real world interactions.

3.1. Models of Trust

Web 2.0 applied previous research on social networks to inject models of communities into the realm of information management. The key idea was to enable peers to share and co-author information. Since most of the solutions that have been delivered are based on the "good will" assumption, the models of trust implemented in Web 2.0 seem too simple to couple with the requirements of identity management.

3.1.1. Simple Model of a Social Network

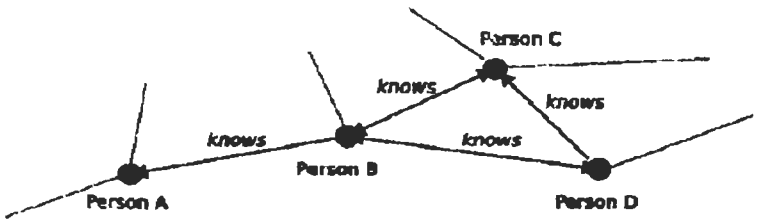
Although the revolutionary six degrees of separation phenomena was published by Milgram in 1967 (30), previous to the Web it has not been applied to the extent that is being applied currently. Online communities, dating services and many more online services are based on the basic concept of social networks. Most online social networks can be modelled as a very simple digraph (or sometimes even a graph) where members of the community are represented as vertices and their mutual relationships as directed/undirected edges (see Definition 1).

Definition 1. Digraph Model of a Social Network. A digraph D_{SN} (m, r: $m \in M_{SN}$, $r \in R_{SN}$) models the social network SN with network members represented as a set of vertices M_{SN} and friendship-relations represented as a set of edges R_{SN}.

The W3C Semantic Web group from Bristol, UK developed the FOAF (10) metadata ontology which captures the basic model of a social network. FOAF is based on the underlying concept of an RDF graph. It maps users (foaf: Agent, foaf: Person) to vertices and relationships (foaf: knows), so that the entire social network can be defined as a list of simple triple-part statements (see Figure 1). Each user is identified by his/her email address (foaf: mbox).

This model of a social network, although very powerful in its simplicity, has certain flaws as previously indicated. Firstly, the only way to define the level of relationship between two users is by the means of degrees of separation (30). Since there is no distinction between a knows relationship and a knows-of relationship, the security constraints of identity management can be compromised by relationships that might be even hostile or corrupt.

Figure 1: Simple Model of a Social Network



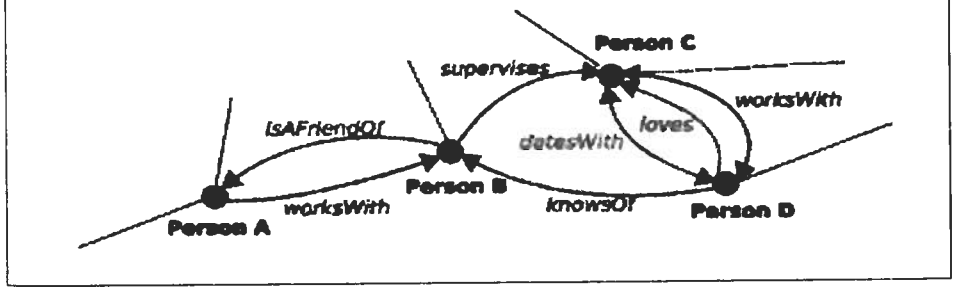
Additionally, the open, distributed approach of RDF allows others to add new triple statements in an uncontrolled manner. These alterations, which can be made without a user's permission (represented by outgoing vertices) are a serious security flaw.

3.1.2. Named Relationships Model

One of the popular features among many community portals is the ability to restrict access to some information by applying simple rules based on the level of a friendship relation. Those levels are usually represented as named relationships derived from the generic concept of the "knows" relationship. orkut[12] allows users to define a relationship type with one of five: best friends, good friends, friends, acquaintances and haven't met, while Flickr[13] defines only three relationships: friend, family member and other. The model of named-relationships can be represented as a graph with coloured edges (11), where different colours represent different types of relationships (see Definition 2). If the set of types of relationships is not exclusive to some kind of relationship (e.g. friendship relations), there might exist more than one different relationship between users and a model of named-relationships would form a multi-graph with coloured edges (see Figure 2).

Definition 2. Coloured Digraph Model of a Social Network. A coloured digraph CD_{SN} (m, r, c: $m \in M_{SN}$, $r \in R(c)_{SN}$, $c \in C$) models the social network *SN* with network members represented as a set of vertices M_{SN} and different types of relationships represented as set of edges $R(c)_{SN}$ coloured with colour c denoting given type of relationship.

Figure 2: Named-Relationship Model of a Social Network



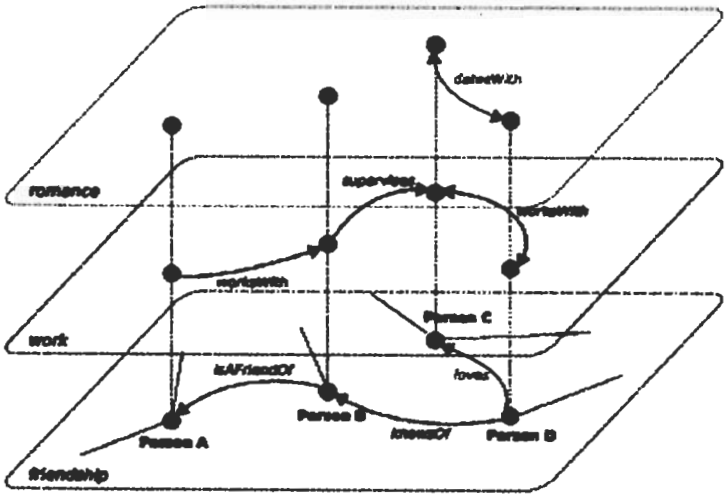
Named relationships are fairly easy to understand and use for community members. But this model can only be applied to information which is not very sensitive such as photographs. One of the reasons for this is that the named-relationships model can be extended beyond a direct relationship. Although services like orkut introduce virtual "friends of my friends" relationships, these solutions might lead to some confusion.

The problem arises even more so when the set of types of relationships can be divided into two or more non-intersecting subsets, representing unrelated types of relationships. This may lead to the creation of multi-domain social networks (see Figure 3) based on given subsets of types of relationships. These overlapping social networks are sparse and further computing trust metrics could be impossible for some parts of the social network graph.

3.1.3. A Simple Model with Relationship Ratings

Named relationships introduce a way of defining the level of relationship between peers. But two issues make named-relationships inadequate for identity management systems:

Figure 3: Multi-Domain Social Network



- Discrete quantification of the friendship levels makes network-wide trust computations difficult;
- Different named-relationships might refer to unrelated concepts, that in particular cases do not introduce ratings of a relationship. Therefore, many simple models of social networks have to be considered independently.

To overcome these problems (28) suggests a normalised float-based relationship rating for the simple model of trust. The graph of relationships then has all relationships annotated with a relationship-level value. This rating allows one to build a simple identity management system incorporating trust delegation, where users can define not only a maximum degrees of separation level but also a minimal trust rating.

A simple relationship rating model of trust (see Definition 3) can be represented by a graph with weighted edges. Each weighted edge represents a direct relationship with ratings provided explicitly by the users themselves. Ratings of relationships between users that are not directly connected have to be computed dynamically (see 3.2), since the social network could change in individual locations dynamically.

Definition 3. Relationship Rating. Each relationship $r \in R_{SN}$ between social network member $m_A \in M_{SN}$ and member $m_B \in M_{SN}$ can have a rating measure FLMcontext $(m_A, m_B) \in < 0, 1 >$ associated with it.

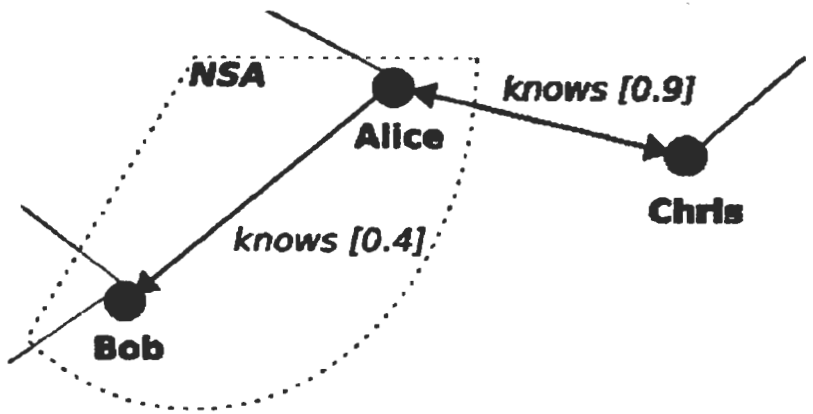
3.1.4. Model of Named-Relationship Ratings

Although a simple relationship rating delivers a robust way to precisely define access control lists, the main problem arises when trying to distinguish between various types of relationships (see Figure 2). A simple relationship rating cannot solve all of the problems which might occur when an identity management system is directed to act in real world fashion.

We move, therefore, to present a scenario where the ratings in a simple relationship model may not be enough (see Figure 4). Let us assume that Alice works for a government agency (NSA) and her work is highly classified. Bob is her co-worker, whom she does not know very well (knows = 40%), but still she has to share this information with him as well as other co-workers directly

connected to her. On the other hand, Chris is her boyfriend, whom she knows very well (knows = 90%), but she cannot reveal the information to him. Since the rating of the relationship between Alice and Bob is lower than that between Alice and Chris, according to a simple relationship rating model, Chris should be granted access to the information Alice has, rather than Bob.

Figure 4: When Simple Model Relationship Ratings are not Enough

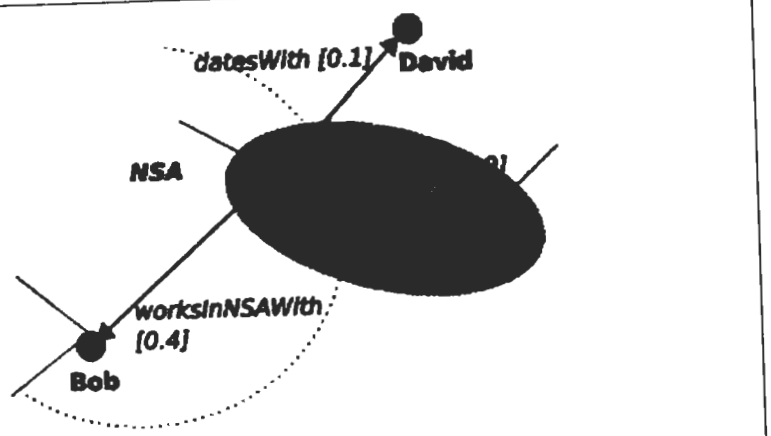


In order to solve this problem we need to combine the named-relationships model with a relationship rating. Then it is possible to distinguish between various types of relationships, such as worksWith and datesWith while at the same time rating them. In our scenario, Alice can protect some sensitive, government information with the constraint being a worksWith relationship. At the same time, some of Alice's private photos can still be protected from being accessed by people that she is not dating (or that she has not built a trust level with to the required extent; see Figure 5).

3.2. Trust Computation

Apart from specifying the model of the social network for the purposes of identity management, essential reliability also depends on the process of trust computations. It will not matter how sophisticated a model of social networking is going to be unless the algorithms used to compute the trust are accurate from a sociological perspective. The user has to have the feeling that the trust metrics

Figure 5: Rating Named-Relationships Model



computed by the identity management system match his/her expectations, otherwise he/she might not be able to precisely specify their access control list.

3.2.1. Dijkstra-Based Trust Computations

One of the easiest methods of computing trust over a social network involves the simple calculation of the distance between nodes in a digraph representing the social network. The most common algorithm is Dijkstra algorithm (18), and as well as the values for the distance between peers, another result of the algorithm is the shortest path from one peer to another. This algorithm can be applied to the measurement of the distance between peers in all models beginning with the most simple one (see 3.1.1).

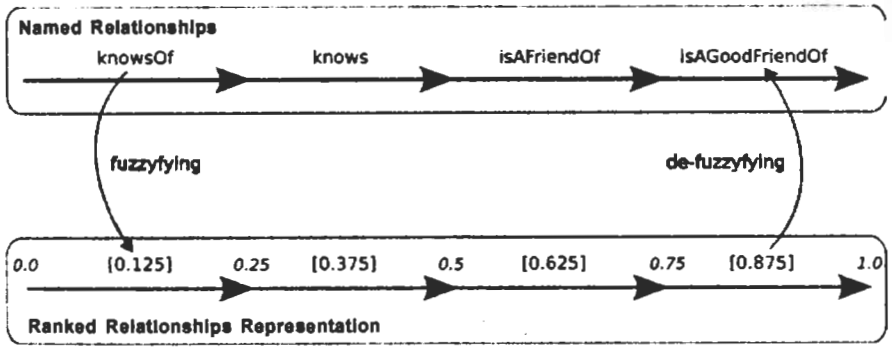
A modified version of the Dijkstra algorithm has been proposed in (28) where the goal of calculating the shortest path has been replaced with the highest friendship ranking value. This algorithm applies to the model of a social network with relationship ratings (see 3.1.3). Since all the relationships are rated with values between 0:0 and 1:0, the modified version of the Dijkstra algorithm multiplies ranking values along the path, and attempts to find the path between two peers with the highest ranking product.

As mentioned already (see 3.1.2), the model of a social network with named relationships introduces some problems for trust computation. To overcome these problems, we propose a simple trust computation algorithm for the named-relationships model of social networks (see Figure 6):

Figure 6: A Simple Trust Computation Algorithm for the Named-Relationships Model of Social Networks

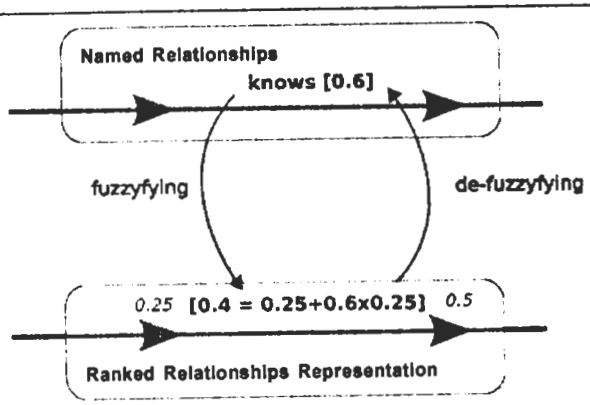
1. Extract multi-domain social networks built with sets of named relationships within a specific domain, for example: friendship, work, romance (see Figure 3).
2. One of the social network domains, based on a specific constraints entry of the access control list, is selected for further computations.
3. All relationship properties that refer to that particular domain of the multi-domain social network are selected, and are (fuzzed) ranked with values between 0:0 and 1:0 that indicates the closeness of the relationship (see Figure 7).
4. Finally, Dijkstra and modified Dijkstra algorithms are used to compute the required trust values.
5. Results from the modified Dijkstra algorithm are translated back (de-fuzzified) to the named relationships.

Figure 7: Fuzzyfying and De-Fuzzyfying Named Relationships



Similar algorithms can be applied to a model of rated named-relationships. The difference is in the fuzzifying and de-fuzzifying process. The ranking values are used to "fuzzify" the discrete values assigned to each named-relationship in the algorithm for the named-relationship model (see Figure 8).

Figure 8: Fuzzyfying and De-Fuzzyfying Named Relationships with Rank Values



Analogous changes are required in the "de-fuzzyfying" process. Although the algorithms for trust computation mentioned above deliver predictable and mathematically-correct results, there is the possibility that they might not reflect the way that users would perceive the actual trust rankings in the real world.

3.2.2. Applying Other Trust Computational Models

We have shown a computational model for the named-relationship amongst individuals. The result of this computation can be applied to other algorithms for trust aggregation in the same overlapping social network.

Moreover, both the fuzzyfying and de-fuzzyfying processes can be extended to almost all existing trust computational models.

For example, the FilmTrust (22) showed how to aggregate the trust values for each individual path and how to use the trust values for a movie recommender system. Our computational model of trust can extend this model to various multiple domain social networks.

3.2.3. Alternative Trust Computations

We have shown how to gain the trust value of a known person. However, this algorithm cannot give any solution regarding an unknown person. For instance, a user joins an online community to learn a new subject. He or she may not know

where to start to form a relationship (and this situation can happen in almost any multi-domain social network or community site).

For this reason, we need to consider the reputation mechanism. The most notable reputation mechanism on the Web was introduced in PageRank (31). The EigenTrust (26) project also proposed a reputation algorithm for a distributed network. It can be used for reputation measuring within social networks along with the fuzzyfying and de-fuzzyfying process.

However, we should consider that a reputation level alone does not capture the full social relationship (see 2.2.1, 2.2.3). The value of a reputation level can help to form a social relationship, but it must not be confused with the value of trust in that relationship.

4. Social Network Management

We have introduced the notion of identity and how to model trust from a social-network perspective. We have described the system requirements as a web-based social network management system and surveyed some potential candidate systems. Finally, we introduced FOAFRealm and described its possible use cases.

4.1. Requirements

We have shown a close connection between the concept of social network and identity. Furthermore, a social network management system cannot be implemented without a complete identity management system.

An identity management system should protect the identity and the privacy of the user within the network. In general, these can be viewed as security features. It is difficult to create a perfectly secure system (especially when identity management system design is usually very security oriented). This is a primary challenge to the social network management system: privacy information should be hidden, yet it must be also available as data on the Web. Security is therefore one of the main problems involved in implementing a social network management system.

How to make a social network system popular is a major difficulty. You must be able to find friends or colleagues on the network if you want to define or form a relationship with them. Many notable systems based on social network methods

have failed for this reason. To create a popular system, it must have the following features: ease of use, capability of adapting to different environments, and the provision of remarkable benefits to the user.

4.2. PGP

PGP is a revolutionary identity management system: it fully satisfies the aforementioned security concerns. However, it has not become popular despite its advanced technology. We will briefly describe why it is not popular and why it cannot be integrated within a social network management system.

- PGP is physically limited by the private key. The private key is not easy for a human to memorise. It cannot be uploaded to a public server. It must be saved to a physical disk of a user. Therefore, it restricts mobility and making it part of the system depends on a physical action of the user.
- PGP is composed of keys. A web based on trust can provide a trust value, but it is difficult to attach more semantic information.
- PGP is not easy to understand or use. This is not trivial matter, and could well be the main reason for its unpopularity.

PGP is also hard to apply to websites. For example, if one website uses PGP as their social network management system, it will require some email interaction (or interaction with other local clients) every time the private key is needed. Moreover, additional user information will be also saved to the webserver. It creates two identities: one restricted to the local machine and another one restricted to the website; a relationship therefore cannot be created without both identities.

4.3. FOAFRealm

Some of the authors have proposed and developed FOAFRealm as a new identity management system for the Web. It is based on a peer-to-peer (P2P) network: a local server saves user profile information and it can communicate with other FOAFRealm-compatible nodes. It also supports a single-sign-on feature that allows a user to use multiple websites with one profile. Security aspects of FOAFRealm are discussed by Grzonkowski (24). We will now describe the merits of FOAFRealm as a social network management system.

- FOAFRealm supports the single-sign-on feature. It gives three advantages.
  - A user can use a FOAFRealm identity within websites.
  - A user does not need to learn how to use a new identity system on future sites.
  - A user is not physically restricted.
- FOAFRealm expresses profile and relationship information based on FOAF and RDF[14] storage. It is straightforward for websites to reuse this information. The profile and relationship information can also be extended.
- FOAFRealm uses the P2P HyperCuP infrastructure[15]. This makes it possible to find and to communicate with other FOAFRealm users on a distributed network: therefore interaction amongst the users is unrestricted by websites or physical disks.

Social Semantic Collaborative Filtering (29) methods have already demonstrated the social networking features of FOAFRealm through a simple relationship rating model. SSCF uses the social network to filter bookmarks of a digital library. A user can find more useful information based on the selections of another trusted user. SSCF techniques have made it not only possible to realise our new model of trust but also to produce an actual use case for a social network.

4.4. Use Cases of Social Network Management

We will now proceed to describe the various use cases for a social network management system. The most attractive use cases are based on user requirements: by creating more relationships among people we can thereby produce a more popular and social system.

The most important use case for social network management is information search and retrieval. In the offline world, information can be propagated by an acquaintance, for example, a book written by a celebrated writer can be promoted through cited references. It is such a real world trust network that we have modelled in our system. The Internet-based social network will accelerate the propagation of trustworthy information (as has already been introduced via the SSCF methods (29). Based on our model, this system can be applied to the searching of other types of information, such as a product in an online shopping mall).

The second use case for social network management is the filtering and ordering of messages. TrustMail demonstrated that a trust network could be used to filter email messages. In our model, the messages will be categorised by multi-domain social networks, and ordered by trust point numbers. For example, a person would notice highlighted messages from trusted colleagues during working hours.

Finally, it can be used to model real communities. A different ACL can be applied to different social networks (see section 3.1.4). A person can use a unique identity to share information within several communities through our model and using FOAFRealm. People need to use a unique identity in order to be a member of overlapping communities. Therefore, this social network management system will be helpful in preventing identity corruption.

5. Trust in a Social Network: The Psychological Point of View

The Oxford English Dictionary (14) defines trust as follows: Confidence in or reliance on some quality or attribute of a person or thing, or the truth of a statement. In fact, trust is often used interchangeably with related words like credibility, confidence or reliability. Trust is the basis for interpersonal interaction and also especially for cooperation within a social network. But there is the question of how we can gain trust.

From the psychological point of view, the answer for this question originates from the theory of human attitudes. The theory specifies attitudes as people's inclination or tendencies to evaluate in positive, neutral or negative ways other people, institutions, activities or even ideas (19). Attitudes consist of three evaluative components. The cognitive component is connected with the opinion or belief segment. Then there is the affective component that is related to emotions or a feeling segment. Finally, there is the behavioral component which is responsible for the intention to behave in a certain way toward someone or something. We could then ask how this theory works in social networks. The affective component begins to operate when we are not able or we have no motivation to perform a rational and detailed evaluation (32). Such situations concern both the real and virtual worlds. It often happens, when we cannot see the other person, that we have no time to perform such an evaluation or sometimes we are not skilled in the domain he/she represents.

If our motivation is slight, and because the result of the aforementioned evaluation was low, we endure the risk that the influence of the affective component will become more ingrained. Therefore, we are prone to using a "liking rule" (17) especially when we reward others for being similar in appearance to us. It takes effect in statements like: He is OK, he is cheerful, but sometimes also: He is annoying, he makes me nervous, I do not like him. Of course, if we take into account only this component, our calculations are very subjective and often are dependent on our momentary state of mind. Although the emotional component seems to be negligible, research findings show that it is of essential importance to the attitude estimation.

When the behavioral component is activated, the attitude is often perceived as the result of every interaction between two interested peers within a social network. If we behave in positive manner, we are more likely to identify our approach favorably. Analogous thinking and negative experiences may lead us to the conclusion that we do not like the other party (15). Although the following examples seem to be paradoxical: I met him, so I like him, they are coherent with respect to cognitive dissonance theory (20). We excuse our own behavior in this manner, because humans want to be rational and consistent when doing things.

While utilising the cognitive component, the user, who gives an opinion, assumes that the emotional relation is based on a rational and knowingly-established reputation about the other peer. If the central path of persuasion (32) is activated, then the attitude towards a virtual friend will be dependent on an analysis of concrete arguments such as reliability or objectivity.

If we take into account the aforementioned psychological aspects, it seems possible to design and implement a computer system that can evaluate the users of a social network. So far, most systems offer only one single summary value that evaluates a specified participant within a network.

The psychological model proposes a distributed estimation of an user. It enables one to minimise the subjectivity of the estimation and force the user to provide a more reliable and systematic manner of estimating each other's participation on the network. In fact, this approach enables one to compare every evaluated person, and thus leads to a more coherent way of evaluating people, which is the fundamental rule that allows one to obtain trust based on perceived evaluations.

6. Conclusions and Future Work

In this article, we have presented methods for trust modelling within social networks in order to match the requirements of community-aware identity management systems.

We have discussed how the trust levels between users can be computed. Finally, we have evaluated our trust models and computation algorithms against recent research in the psychology domain.

We have described that the trust level of users relies on the separate social networks that they are members of. However, there is still the possibility that the trust levels of two or more social networks can be related. The meaning of their conjunction, its model and computation, will be explored in our future work.

Another issue to look at is that of the trust and identity of other objects apart from people (e.g. trusted computers, resources, etc.). The work presented in this paper can be easily extended to express trust between and identity of both machines and people (by referencing foaf: Agent as well as foaf: Person), but more effort is required to extend our methods to other concepts such as websites or documents.

In addition to, the FOAFRealm project has initiated work on a novel DigiMe system (27). Compatible with Identity 2.0 protocol (13), this future work will give users full control over their virtual identities and the ability to describe their online relationships in manner close to the real world. Furthermore, we will take advantage of Service Oriented Architecture (SOA) paradigns to create a mobile client version of FOAFRealm, thereby enabling ubiquitous user profile manipulation.

7. Acknowledgments

This material is based upon works supported by Science Foundation Ireland under grant no. SFI/02/CE1/I131, partially by the EU FP6 Knowledge Web project under project no. 507482, by KBN, Poland under grant no. 4T11C00525, and by the Ministry of Information and Communication in the Republic of Korea's National Project for Information Technology Advancement. The authors would like to thank Stefan Decker and Hong-Gee Kim for sharing their thoughts on trust modelling in social networks and Suk-Hyung Hwang and Siegfried Handschuh for all their help.

(Hee-Chul Choi, DERI, Seoul National University, Korea. He can be reached at heechul.choi@deri.org

Sebastian Ryszard Kruk, DERI, NUI Galway, IDA Business Park, Lower Dangan, Galway, Ireland. He can be reached at sebastian.kruk@deri.org

Slawomir Grzonkowski, WETI, Gdansk University of Technology, Narutowicza 11/12 Gdansk, Poland. He can be reached at slawomir.grzonkowski@deri.org

Katarzyna Stankiewicz, WZIE, Gdansk University of Technology, Narutowicza 11/12 Gdansk, Poland. He can be reached at kst@zie.pg.gda.pl

Brian Davis, DERI, NUI Galway, IDA Business Park, Lower Dangan Galway, Ireland. He can be reached at brian.davis@deri.org

John G Breslin, DERI, NUI Galway, IDA Business Park, Lower Dangan Galway, Ireland. He can be reached at john.breslin@deri.org)

Endnotes

1 *http://gmail.google.com*
2 *http://www.orkut.com*
3 *http://isnoop.net/gmail*
4 *http://www.naver.com, http://empas.com*
5 *http://www.google.com*
6 *http://www.phpbb.com/*
7 *http://www.vbulletin.com*
8 *http://rdfs.org/sioc*
9 *http://www.ecademy.com/*
10 *http://www.yubnub.org/*
11 *http://del.icio.us*
12 *orkut: http://www.orkut.com/*
13 *Flickr: http://www.flickr.com/*
14 RDF: *http://www.w3.org/RDF*
15 Lightweight HyperCuP implementation project: *http://www.hypercup.org/*

References

1. e-Bay: *http://www.ebay.com/.*
2. *http://trusted-systems.info/.*
3. *http://global-info-society.org/.*
4. *http://worldpolicy.org/.*
5. PGP Specification: *http://www.ietf.org/rfc/rfc1991.txt.*
6. An Open Specification for Pretty Good Privacy: *http://www.ietf.org/html.charters/openpgp-charter.html.*
7. PKI working group: *http://www.ietf.org/html.charters/pkix-charter.html.*
8. TrustMetrics Wiki: *http://moloko.itc.it/trustmetricswiki/moin.cgi/PaperTrustMetricsSurvey.*
9. PeerTrust Homepage: *http://www-static.cc.gatech.edu/projects/disl/PeerTrust/.*
10. FOAF Vocabulary Specification: *http://xmlns.com/foaf/0.1/.*
11. *http://planetmath.org/encyclopedia/.*
12. FOAFRealm project: *http://www.foafrealm.org/.*
13. Identity 2.0: *http://www.identity20.com/.*
14. Oxford English Dictionary, page 3423. New York: Oxford University Press, the compact edition, 1971.
15. D J Bem. "Self-perception theory." In L Berkowitz, editor, *Advances in Experimental Social Psychology*, volume 6, pages1-62. Academic Press, New York, 1972.
16. L J Camp. "Designing for trust." *In Trust, Reputation, and Security*, pages 15-29, 2002.
17. R B Cialdini. "Influence: Science and practice." Allyn and Bacon, Boston, MA, 2001.
18. E W Dijkstra. A note on two problems in connexion with graphs. *Numerische Mathematik*, 1:269-271, 1959.
19. A H Eagly and S Chaiken. "The psychology of attitudes." Fort Worth, TX: Harcourt Brace Jovanovich College Publishers, 1993.
20. L Festinger. "A Theory of Cognitive Dissonance." Stanford University Press, 1957.
21. L Garton, C Haythornthwaite, and B Wellman. Studying online social networks. *J Computer-Mediated Communication*, 3(1), 1997.
22. J Golbeck and J Hendler. "Filmtrust: Movie recommendations using trust in web-based social networks." In Proceedings of the Consumer Communications and Networking Conference, 2006.
23. J Golbeck, B Parsia, and J Hendler. "Trust networks on the semantic web." In Proceedings of Cooperative Intelligent Agents, *http://www.mindswap.org/papers/CIA03.pdf*, 2003.
24. S Grzonkowski, A Gzella, H Krawczyk, S R Kruk, F J M-R Moyano, and T Woroniecki. "D-FOAF – Security Aspects in Distributed User Management System." In TEHOSS'2005.

25. A Josang. "An algebra for assessing trust in certification chains." In NDSS, 1999.

26. S D Kamvar, M T Schlosser, and H Garcia-Molina. "The eigentrust algorithm for reputation management in P2P networks." 2003.

27. S R Kruk. Digime – personalization vs privacy. *http://skruk.blogspot.com/2006/02/digime-personalization-vs-privacy.html.*

28. S R Kruk. "FOAF-Realm – control your friends' access to the resource." In FOAF Workshop proceedings, *http://www.w3.org/2001/sw/Europe/events/foaf-galway/papers/fp/foaf realm/*, 2004.

29. S R Kruk and S Decker. "Semantic social collaborative filtering with foafrealm." In Semantic Desktop Workshop, ISWC 2005, 2005.

30. S Milgram. "The small world problem." *Psychology Today*, 67(1), 1967.

31. L Page, S Brin, R Motwani, and T Winograd. "The pagerank citation ranking: Bringing order to the web." Technical Report SIDL-WP-1999-0120, Stanford University, Nov. 1999.

32. R Petty and J Cacioppo. *The Elaboration Likelihood Model of persuasion*. New York: Academic Press, 1986.

33. L von Ahn, M Blum, N J Hopper, and J Langford. "Captcha: Using hard AI problems for security." In *EUROCRYPT*, pages 294-311, 2003.

34. L Xiong and L Liu. "Building trust in decentralized peer-to-peer electronic communities." In Fifth International Conference on Electronic Commerce Research (ICECR-5), 2002.

35. J Yen, R Popp, G Cybenko, L Sweeney, K Taipale, and P Rosenzweig. Homeland security. *IEEE Intelligent Systems*, 20(5): 76-86, 2005.

36. P Zimmermann. *Pretty good privacy user's guide*, volume I and II. 14th June 1993 Revision, Distributed with the PGP software, 1993.

8

On Helping Individuals to Manage Privacy and Trust

Stephen Crane, Marco Casassa Mont and Siani Pearson

Being able to say with absolute certainty that another party can be trusted to handle personal information with today's technology is probably unrealistic. In this paper we explain an approach to establishing trust, based on the status of a remote platform and an anticipated willingness of the other party to comply with prior negotiated obligations. Ongoing monitoring and notification, and the ability of the individual to form a simple record of past interaction, provides the individual with greater confidence in situations where they need to share personal sensitive information with organisations they would otherwise not be able to claim they trust. We describe the principles of our approach and architectures that support a practical implementation.

1. Introduction

Within PRIME[1,2,3] we have been investigating how Personal Identifying Information (PII) can be shared between one individual to other individual, and between individual and an organization, in a way that reassures the individual,