2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications

Fine-Grained Trust Assertions for Privacy Management in the Social Semantic Web

Owen Sacco, John G. Breslin and Stefan Decker
Digital Enterprise Research Institute,
National University of Ireland, Galway
owen.sacco@deri.org, john.breslin@nuigalway.ie and stefan.decker@deri.org

***Abstract*—Social Web applications are engineered around users sharing personal information with their connected peers. They provide generic privacy settings which user specify with whom their information can be shared. However, this does not model the real world where one might trust someone with specific personal data but not with other data. Therefore, trust has to be taken into consideration when applying privacy settings. In our previous work, we modelled fine-grained privacy preferences without asserting trust. In this work, we add trust to our Privacy Preference Framework to provide more fine-grained enforcement of access control when sharing information. This ensures that users' personal information is accessed only by the intended third parties.**

***Keywords*-Access Control, Privacy, Trust, PPO, PPM, TAO, Social Semantic Web, Web of Data.**

I. Introduction

Online Social Networks have become part of our lives where we store, manage and share personal information about ourselves with other users online. We build connections in social networks based on life events such as people we have met and interacted with at college, work, conferences, acquaintances and even our close relatives.

However, in real life, we do not share all our private information with everyone but we only share parts of our information to whom we trust based on several factors such as past interactions, the type of relationship, similar personality attributes such as interests, the sensitive nature of the information we are sharing at that moment in time and so forth. Whilst Online Social Networks provide generic privacy settings, these privacy settings are not fine-grained [2] and do not take trust into consideration.

In this paper, we focus on adding trust to our Privacy Preference Framework [17] whereby trust judgements are asserted for each entity requesting user personal information. We focus on using various methods to automatically assert fine-grained subjective trust values for different social factors such as profile similarity and reputation in trusted networks; as opposed to other work on trust that only focus on one social factor and heavily involve users to enter their trust judgements [1]. We also demonstrate how privacy preferences are enforced based on this fine-grained subjective trust value that would provide further control when sharing personal data.

The remainder of this paper is organised as follows: section II provides scenarios where trust is a concern. Section III provides several definitions of trust and explains several social factors that effect trust judgements. Section IV explains the methods used to assert subjective trust values for each social factor used in our work. In section V, the Trust Assertions Ontology (TAO) is presented which is used for modelling and storing the asserted subjective trust values from each social factor. Section VI defines Information Confidentiality, our new approach to managing personal information by defining the confidentiality level for each specific personal information. Section VII presents the implementation for asserting trust as enhancements in the Privacy Preference Manager [14] to filter data based on information confidentiality and the asserted subjective trust values. Section VIII outlines our experiment and results for assessing subjective trust judgements. Section IX discuses related work and section X presents future work and concludes the paper.

II. Motivations

Present Social Networks provide generic privacy settings that grant or deny access to users that are in one's social graph. Although user lists can be created and privacy settings can be applied to these user lists, current Social Networks assume that all users share the same amount of trust. Despite the fact that one can manually specify who can access personal information, this is a tedious task when in most cases users are connected to a large number of peers. Moreover, although there are applications that export user's personal information from closed Social platforms, the privacy settings are platform dependent that cannot be exported and reused on other platforms.

Therefore a system is required that exports and aggregates information from various Social Web applications into a Social Semantic Web platform; consisting of aggregated personal information which is annotated with contextual meaning and formatted in RDF. This system will use the Privacy Preference Manager that provides users to specify fine-grained privacy preferences on the aggregated data and it could push back filtered information to the respective Social Web application through their APIs. When filtering

This work is funded by the Science Foundation Ireland under grant number SFI/08/CE/I1380 (Líon 2) and by an IRCSET scholarship co-funded by Cisco systems.

978-0-7695-5022-0/13 $26.00 © 2013 IEEE
DOI 10.1109/TrustCom.2013.30

personal information, the Privacy Preference Framework will also automatically assert trust judgements similar to trust judgements one would make in real life. The system would provide users to set a trust threshold to their personal information so that only those who are above this threshold and that satisfy the privacy preferences would be granted access to the personal information.

III. Defining Trust

Trust judgements are very subjective and depends on the person's perception when determining a trust decision at a point in time in a specific context. Therefore, trust can have several meanings depending (1) who is making the trust judgement, (2) on what the trust judgement is being made and (3) the context at which the decision is carried out.

A. Meaning of Trust

Most literature review on trust differ when defining the meaning of trust. The authors in [8] define trust as a belief in the entity's competence to act within a specified context. However, the authors in [11] state that trust depends on the actions themselves rather than on the competences and define trust as a measurable belief on one party to another for a particular service that the other party behaves faithfully during a specified time within a specified context.

In this paper, trust depends on a person's subjective belief at that point in time s/he is sharing information that another person will act responsibly and will not misuse the information. Moreover, we assume that trust is asymmetric and users do not trust each other in the same way. Therefore, our meaning of trust is similar to the author's definition in [11], but with relation to personal information rather than services.

B. Modelling Trust

A model is required to quantify and express the subjective trust values. Similar to the trust model in [10] and [9], subjective trust values are represented in the range of [-1,1] where the range boundaries define: a subjective trust value of 1 represents absolute trust in the entity's information, -1 represents absolute distrust, and values in between the range define subjective trust values of trust or distrust. The subjective trust value 0 represents either uncertainty or unknown due to a lack of information that the trust value could not be asserted. Positive values less than 1 still represent trust but it represents that there is an element of uncertainty or unknown information rather than absolute trust. This also applies to negative values that represent distrust.

Subjective trust values are the result of assertions of a user's subjective belief of an entity in a Social Web application for a particular social factor.

C. Social Factors that effect Trust Judgements

Trust depends on several social factors such as trust is gained over time through past interactions with a person, opinions of a person's actions, other people's opinions, rumours, psychological factors impacted over time, life events and so on. Asserting trust based on all of these factors in Social Networks can be hard to compute since the information required is limited and not available [4]. However, we outline several factors that can be used to assert trust with the information in current Social Web applications: (1) identity of the requester: trust can be asserted from the credentials exchanged through authentication, (2) profile similarity between the user and the requester: trust can be asserted by matching several profile attributes with one another, (3) the relationship type between the user and the requester: trust can be asserted based on the importance of the relationship type, (4) the reputation of the user within a trusted network: trust can be asserted through reputation information asserted from other entities in a Web of Trust, (5) trust based on interactions between the user and the requester: trust can be asserted based on the number of interactions between the user and the requester over a particular period of time.

A subjective trust value is asserted from each social factor outlined above and an average of the sum of all subjective trust values is then calculated to represent the user's subjective trust value of a requester. The next section explains in detail our methods to assert subjective trust values from each social factor.

IV. Trust Assertions

Current work on trust only focus on one social factor, but since in real life many social factors are normally used by a user to determine whether a requester is trusted, in our work we use all of the above mentioned factors to assert a fine-grained social-based subjective trust value for the requester at the time s/he requests the data.

The assertions are calculated on the aggregated profiles of the user and of the requester. These contain profile information and activity information from various Social Web platforms the user and the requester are subscribed to. These profiles are aggregated, matched, curated and defined in RDF using various vocabularies such as Friend-of-a-Friend (FOAF)[1] for describing basic personal information, the Relationship Ontology[2] for describing relationship types with other users, the Description-of-a-Career (DOAC)[3] for describing career related information and Semantically Interlinked Online Communities (SIOC)[4] for describing activities within the Social Web platform such as sharing of microblog

[1]FOAF — http://www.foaf-project.org
[2]Relationship — http://vocab.org/relationship/.html
[3]DOAC — http://ramonantonio.net/doac/0.1/
[4]SIOC — http://sioc-project.org/

post. In order to disambiguate terms such as user's interests, DBPedia[5] concepts are used to describe such terms. Techniques such as in [12] are used to model and aggregate user profiles, however user modelling is beyond the scope of this research paper.

A. Identity-based Trust

Identity relies on authentication whereby a user is identified after s/he successfully provides correct credentials to a system. In Social Web applications, users provide a username and password in order to authenticate themselves into the system. Currently, most Social Web applications provide Single Sign-On (SSO) mechanisms, such as OpenID[6] whereby one authenticates on one platform which confirms the user's identity to other Web applications.

In Semantic Web applications, the WebID protocol [18] can be used as a Single Sign-On service to identify users. It provides a mechanism whereby users can authenticate using FOAF and X.509 certificates over SSL. The digital certificates contain the public key and a URI that points to the location where the FOAF profile is stored. The authentication mechanism parses the WebID URI from the certificate and retrieves the FOAF profile from its location. The public key in the certificate and the public key in the FOAF profile are checked to grant the user access if the public keys match.

The WebID certificates can be self-signed certificates. However, to ensure more trustworthiness of users, we encourage that the certificates are issued by trusted Certificate Authorities (CA) since it is the CAs responsibility to verify the user's identity before binding them to their respective public key.

The subjective trust value is assigned to the requester after s/he authenticates using WebID. If successful, then the requester is assigned 1, if unsuccessful the requester is assigned -1 and 0 if the process is aborted. The trust value cannot be a value in between the range [-1,1] since either authentication is successful or not.

Definition 1: Identity-based trust. Let IDT be the subjective trust value for identity, $Cert$ an SSL digital signed certificate, R a requester identified by a URI, RP a requester's FOAF profile and U a user identified by a URI. Let $Certificate(Cert, R)$ mean that $Cert$ is the SSL certificate of R, $Profile(RP, R)$ mean that RP is the profile of R, $Verify(Cert, RP)$ mean that the public key in $Cert$ is verified with the public key in RP, $AssertedBy(R, U)$ mean that R is asserted by U and $AssignTrust(IDT, R)$ mean that R is assigned IDT, where $IDT \in \{-1, 0, 1\}$. Thus, Identity-based trust is defined:

$$\textit{Certificate(Cert,R)} \wedge \textit{Profile(RP,R)} \wedge \textit{Verify(Cert,RP)} \wedge \textit{AssertedBy(R,U)} \Rightarrow \textit{AssignTrust(IDT,R)} \quad (1)$$

B. Profile Similarity-based Trust

Profiles contain information about users and consists of basic information such as name and surname, contact details such as e-mail addresses, user's interests, connected peers including their specific relationship types, projects the user is working on, activities the user is engaged in such as sharing of microblog posts and so forth.

In [4], the authors explain the importance of asserting trust between similar profiles of different users as they claim that "the more similar two people were, the greater the trust between them". However, the authors do not assert trust on similarity between profile attributes. Therefore, we assert trust by observing the similarity between the user's profile and the requester's profile by comparing the distinct attributes that are common in both profiles. The basic information attributes are not taken into consideration as these are different for each user. However, attributes such as work place information, interests, projects, connected peers and other profile attributes are compared. Hence, we compute the subjective trust value for profile-similarity by calculating the relationship between the sum of matched distinct profile attributes between the user's profile and the requester's profile, and the total sum of all the distinct attributes within the user's profile. This calculation is represented with the following formula:

$$\tau = \frac{\sum_{i=1}^{n} m_i}{\sum_{i=1}^{n} a_i} \quad (2)$$

where τ denotes profile similarity subjective trust value, m denotes the matched distinct profile attributes between the user's profile and the requester's profile, and a denotes the user's distinct profile attributes.

Definition 2: Profile Similarity-based trust. Let PST be the subjective trust value for profile similarity, R a requester identified by a URI, RP a requester's FOAF profile, RA a requester's profile attribute, U a user identified by a URI, UP a user's FOAF profile and UA a user's profile attribute. Let $Profile(RP, R)$ or $Profile(UP, U)$ mean that RP is the profile of R or UP is the profile of U, $Contain(RA, RP)$ or $Contain(UA, UP)$ mean that RA is within profile RP or UA is within profile UP, $Match(RA, UA)$ mean that RA is matched with UA, $AssertedBy(R, U)$ mean that R is asserted by U and $AssignTrust(PST, R)$ mean that R is assigned PST, where $PST \in [-1, 1]$. Thus, Profile Similarity-based trust is defined:

[5]DBPedia — http://dbpedia.org/
[6]OpenID – http://openid.net/

$$\forall UA(Profile(RP,R) \wedge Profile(UP,U) \wedge Contain(RA,RP) \wedge Contain(UA,UP) \wedge Match(RA,UA) \wedge AssertedBy(R,U)) \Rightarrow AssignTrust(PST,R) \quad (3)$$

C. Relationship-based Trust

Social Web platforms provide users to define specific relationship types that describe the connection between two users such as family members. These can easily be modelled using the Relationship Ontology when aggregating information. However, it is quite hard to model the importance of these relationship types as there is no information that denotes which relationship type is more important than another. Therefore, the Social Semantic Web application provides the user the option to enter a value of how much s/he trusts that particular relationship type. The value must be within the range [-1,1].

Definition 3: Relationship-based trust. Let RLP be the subjective trust value for relationship types, R a requester identified by a URI, U a user identified by a URI, UP a user's FOAF profile and URT a user's relationship. Let $Profile(UP, U)$ mean that UP is the profile of U, $Contain(URT, UP)$ mean that URT is within profile UP, $Relationship(R, URT)$ mean that R is in the relationship URT, $AssertedBy(R, U)$ mean that R is asserted by U and $AssignTrust(RLP, R)$ mean that R is assigned RLP, where $RLP \in [-1, 1]$. Thus, Relationship-based trust is defined:

$$\forall URT(Profile(UP,U) \wedge Contain(URT,UP) \wedge Relationship(R,URT) \wedge AssertedBy(R,U)) \Rightarrow AssignTrust(RLP,R) \quad (4)$$

D. Reputation-based Trust

The majority of Social Web applications offer services based on connections amongst peers which form a social graph. The nodes in the graph represent users and the edges represent the connections between the users within a directed graph.

Reputation-based trust consists of a trust measurement of a user within this graph based on all trust values which users give amongst each other. These trust ratings about other users create a "Web of Trust" [5]. Since a user's reputation trust value depends on trust ratings from others, the trust rating of the person giving a trust rating to another entity must also be taken into consideration. Therefore, we assert reputation-based trust value as the weighted average value of all trust values given to a user[7]. The weighted average consists of the user's trust values assigned within a network and the weights for each trust value denotes the reputation value of the person that assigned the trust value. The reputation-based trust assertion is represented with the following formula:

$$\bar{\tau} = \frac{\sum_{i=1}^{n} w_i v_i}{\sum_{i=1}^{n} w_i} \quad (5)$$

where $\bar{\tau}$ denotes reputation trust, w denotes the reputation of the user assigning a subjective trust value to the requester and v denotes the requester's subjective trust value assigned by a user.

Definition 4: Reputation-based trust. Let RPT be the subjective trust value for reputation, R a requester identified by a URI, RV requester's reputation value, U a user identified by a URI and SG a social graph. Let $SocialGraph(SG, U)$ mean that SG is the social graph of U, $Contain(R, SG)$ mean that R is in SG, $Measure(RV, SG)$ mean that RV is measured in SG, $Reputation(RV, R)$ mean that RV is the reputation value of R, $AssertedBy(R, U)$ mean that R is asserted by U and $AssignTrust(RPT, R)$ mean that R is assigned RPT, where $RPT \in [-1, 1]$. Thus, Reputation-based trust is defined:

$$SocialGraph(SG,U) \wedge Contain(R,SG) \wedge Measure(RV,SG) \wedge Reputaion(RV,R) \wedge AssertedBy(R,U) \Rightarrow AssignTrust(RPT,R) \quad (6)$$

E. Interactions-based trust

Interactions consists of users sharing microblog posts, comments, photos, videos, links and other shareable content specifically with their connected peers. Social Web platforms allow users to extract these interactions through their APIs and this information can be described using the SIOC vocabulary. It is the norm that users interact with those users who they trust most and therefore trust can be asserted based on the amount of interactions one has with another. Therefore, we compute the subjective trust value for interactions by calculating the relationship between the sum of interactions between the user and the requester, and the total sum of all the interactions of the user. This calculation is represented with the following formula:

$$\tau = \frac{\sum_{i=1}^{n} r_i}{\sum_{i=1}^{n} u_i} \quad (7)$$

where τ denotes interactions trust, r denotes the number of interactions between the requester and the user, and u denotes the number of all the user's interactions in the Social Web platform.

Definition 5: Interactions-based trust. Let $INTT$ be the subjective trust value for interactions, R a requester identified by a URI, U a user identified by a URI,

[7]The trust value can be asserted using Profile Similarity-based trust method or a combination of other methods.

UP a user's FOAF profile and UI a user's interaction. Let $Profile(UP, U)$ mean that UP is the profile of U, $Contain(UI, UP)$ mean that UI is within profile UP, $Interaction(R, UI)$ mean that R is in the interaction UI, $AssertedBy(R, U)$ mean that R is asserted by U and $AssignTrust(INTT, R)$ mean that R is assigned $INTT$, where $INTT \in [-1, 1]$. Thus, Interactions-based trust is defined:

$$\forall UI(Profile(UP,U) \wedge Contain(UI,UP) \wedge Interaction(R,UI) \wedge AssertedBy(R,U)) \Rightarrow AssignTrust(INTT,R) \quad (8)$$

F. Aggregating Subjective Trust Values

In order to assign a fine-grained user's subjective trust value to a requester, we calculate an average of all the subjective trust values of a requester from each social factor assigned by the user. This calculation is represented by the following formula:

$$\tau = \frac{1}{n} \sum_{i=1}^{n} s_i \quad (9)$$

where τ denotes the aggregated subjective trust value and s a subjective trust value asserted based on a social factor.

Definition 6: Aggregate Subjective Trust. Let AT be the aggregated subjective trust value, R a requester identified by a URI, U a user identified by a URI, IDT be the subjective trust value for identity, PST be the subjective trust value for profile similarity, RLP be the subjective trust value for relationship types, RPT be the subjective trust value for reputation and $INTT$ be the subjective trust value for interactions. Let $Assigned(IDT, R)$ mean that IDT is assigned to R, $Assigned(PST, R)$ mean that PST is assigned to R, $Assigned(RLP, R)$ mean that RLP is assigned to R, $Assigned(RPT, R)$ mean that RPT is assigned to R, $Assigned(INTT, R)$ mean that $INTT$ is assigned to R, $AssertedBy(R, U)$ mean that R is asserted by U and $AssignTrust(AT, R)$ mean that R is assigned AT, where $AT \in [-1, 1]$. Thus, the Aggregate Subjective Trust is defined:

$$Assigned(IDT,R) \wedge Assigned(PST,R) \wedge Assigned(RLP,R) \wedge Assigned(RPT,R) \wedge Assigned(INTT,R) \wedge AssertedBy(R,U) \Rightarrow AssignTrust(AT,R) \quad (10)$$

V. Trust Assertion Ontology (TAO)

The Trust Assertion Ontology illustrated in figure 1 — http://vocab.deri.ie/tao# — is a light-weight vocabulary to describe user's subjective trust values for requesters. The subjective trust values are stored for later retrieval so that the system only needs to compute the total average sum of all asserted trust values at run time unless there are any updates in any of the profiles. The classes and properties provided by TAO are defined below:

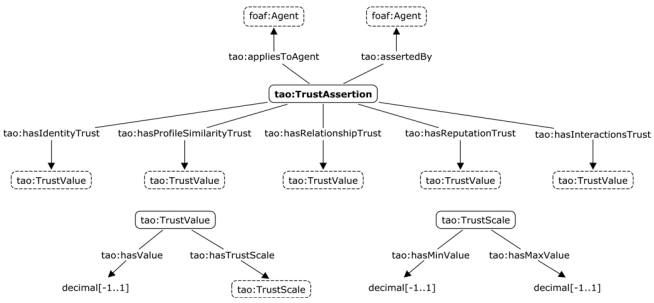

Figure 1. The Trust Assertion Ontology (TAO)

- `tao:appliesToAgent` specifies an agent who the subjective trust values are about.
- `tao:assertedBy` specifies an agent who assigned the trust values.
- `tao:hasIdentityTrust` specifies the subjective trust value based on the requester's identity.
- `tao:hasProfileSimilarityTrust` specifies the subjective trust value based on the profile similarity between the user and the requester.
- `tao:hasRelationshipTrust` specifies the subjective trust value based on the relationship type between the user and the requester.
- `tao:hasReputationTrust` specifies the subjective trust value based on the requester's reputation in a social network.
- `tao:hasInteractionsTrust` specifies the subjective trust value based on the number of interactions between the user and the requester.
- `tao:TrustValue` is a class that specifies the subjective trust value within a trust scale.
- `tao:TrustScale` is a class that specifies the minimum and maximum subjective trust values.

VI. Information Confidentiality

Our work focuses on determining whether the subjective trust value of a requester satisfies a trust threshold which a user specifies for each part of the information being requested. We propose a novel approach whereby the user gives a weighted value to each part of his/her information that represents the confidentiality level, i.e. how sensitive and important that information is to the user. Therefore, in order to determine whether a requester can access the requested information, the requester's subjective trust value is checked whether it is equal or greater than the confidentiality value given for that information. This confidentiality level, known as *Information Confidentiality*, can be modelled within a privacy preference described using the Privacy Preference Ontology (PPO).

```
[...]
ppo:appliesToResource <owen.sacco@deri.org>;
ppo:hasConfidentiality [
   wo:weight_value "0.8"; wo:scale pposcale1 ];
[...]
```

Figure 2. Information Confidentiality

A. Overview of the Privacy Preference Ontology (PPO)

The Privacy Preference Ontology (PPO) ([13], [15]) - is a light-weight Attribute-based Access Control (ABAC) vocabulary that allows users to describe fine-grained privacy preferences for restricting or granting access to non-domain specific Linked Data elements, such as Social Semantic Data.

As PPO deals with RDF(S)/OWL data, a privacy preference, defines: (1) the resource, statement, named graph, dataset or context it must grant or restrict access to; (2) the conditions refining what to grant or restrict (3) the access control privileges; and (4) a SPARQL query, (`AccessSpace`) *i.e.* a graph pattern representing what must be satisfied by the user requesting information.

B. Extending PPO with Information Confidentiality

Modelling information confidentiality requires the following: (1) which specific information to assign the information confidentiality value to; (2) the information confidentiality value; and (3) the access control privilege granted if the information confidentiality value is satisfied. We have extended PPO with a property called `ppo:hasConfidentiality` that defines the information confidentiality value within the range between [0,1]. The boundaries for the information confidentiality values are: 0 being non-confidential and 1 being highly confidential.

A privacy preference with information confidentiality will read *"grant access to my personal e-mail address if a requester's trusted value satisfies the information confidentiality value of* x*"*, where x being a value within the range [0,1]. This is described using PPO as illustrated in figure 2.

VII. Implementing Trust Assertions

The Privacy Preference Framework consists of the Privacy Preference Manager (PPM) ([14], [16], [17]) which was developed to implement the creation of privacy preferences for RDF data described using PPO and to filter requested data by enforcing the privacy preferences. We have extended the Privacy Preference Framework with the addition of a Trust Manager (TM) component that asserts trust values using methods as defined in section IV before the privacy preferences are enforced by the PPM. Although the whole architecture is designed to work with any Semantic Data, in this paper we focus on requesting personal information from FOAF profiles. With FOAF profiles, our aim is to illustrate how personal information can be filtered based on asserting subjective trust values for requesters in relation to the FOAF profile owner and to the information being requested.

The PPM is a Web application and a user can either create an instance on a central server or can opt to install their own instance in a Federated Social Web scenario. It acts as a filter mechanism for RDF stores or any other RDF data. It filters user's personal information when a third party user sends a request or SPARQL query through the interface or the API. The PPM has been extended so that it allows users to: (1) authenticate using WebID to their instance and create privacy preferences including information confidentiality preferences for their private information, and (2) authenticate using WebID to other user's instance and request personal information.

The Privacy Preference Manager's user interface was extended to provide the data owner with the option to add the information confidentiality value and also to add the relationship trust values.

The sequence in which the Privacy Preference Framework enforces the privacy preferences has been extended so that it can assert the user's subjective trust values for the requester. The sequence, as illustrated in figure 3, is as follows: (1) a requester authenticates to the Privacy Preference Framework using WebID and requests for a user's particular information through options or through SPARQL queries from the interface[8]; (2) the user interface sends the request to the Trust Manager; (3) the Trust Manager first queries the Trust Assertion store (which stores the subjective trust values defined using TAO) and checks whether trust values have already been computed for the requester; (4) if the Trust Assertion store does not contain any trust values, the Trust Manager asserts the subjective trust values from the requester's profile[9], updates the Trust Assertion store with the subjective trust values and sends the aggregated subjective trust value to the enforcer module; (5) the enforcer module evaluates whether the subjected trust value satisfies the information confidentiality value for the requested data and it also enforces the privacy preferences (if any) that relate to the requested data; (6) if any of the information confidentiality values and privacy preferences relating to the requested data are satisfied, the filtered data is sent to the requester.

VIII. Experiment and Results

In order to examine the trust assessments based on Social data we conducted an experiment whereby we extracted 15 user profiles from Facebook, LinkedIn and Twitter. The extracted information include the following: (1) Basic Information: full name, date of birth, age and gender; (2) Contact Information: email addresses, phone numbers and mobile

[8]The Privacy Preference Framework provides an API so that other applications can send SPARQL queries.

[9]The Trust Manager communicates with the WebID module to assert the Identity subjective trust value.

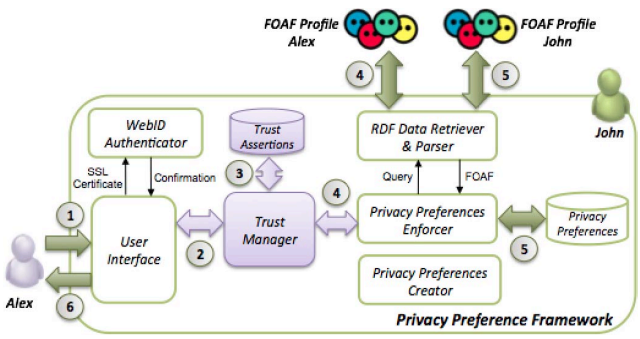

Figure 3. Asserting Trust in the Privacy Preference Framework

phone numbers; (3) Personal websites; (4) Affiliations: website of the user's work place; (5) Online Accounts: example Twitter ID, LinkedIn ID and Facebook ID; (6) Education: user's educational achievements and institutes from where these achievements were obtained; (7) Experiences: job experiences including job title and organisation; (8) Interests: user interests; (9) Interactions: direct microblog posts to other users (that containt text, photos, videos, URL links or any other content); and (10) Relationships: connected users (i.e. friends), relationship types and relationship statuses.

These profiles were aggregated and transformed into RDF using common vocabularies as explained in the previous sections. The users are all co-workers and each co-worker is connected to each other that form a trusted network. A WebID certificate for each user was created and a Privacy Preference Manager instance for each user was also created.

The users were required to set the information confidentiality level for each specific part of their profile data and also to set the trust level for their relationship types.

The subjective trust values for each user (based on the methods as explained in section IV) were computed. As an example, table I illustrates user 1's subjective trust values of the other 14 users in this trusted network. The subjective trust values are stored[10] in the Trust Assertions store described in TAO. With these values, the privacy preference manager checks whether the aggregated trust value satisfies the confidentiality level for any requested information. Therefore, each of the other 14 users will only have access to the information which their aggregate trust value satisfies user 1's information confidentiality level for each specific information.

IX. Related Work

Most current work on trust in Social Networks focus on users giving rating scores to other peers. The authors in [3] focus on recommending films based on trust ratings from Social Networks. The authors apply their work to their social network called FilmTrust. They use the algorithm called TidalTrust for recommending movies based on trust values and based on the social network structure. Although the authors use social trust, the trust ratings are manually assigned by users and their work focuses only on information from a single Social Network. In contrast, our work focuses on automatically asserting trust from information extracted from various Social Web applications.

In [5] the authors focus on inferring trust and reputation in Social Networks. The trust ratings are assumed to be inputted by users. These values represent trust values about other users to whom they are connected to. Although they provide beneficial algorithms to infer trust from links in Social Networks, this work still relies on ratings manually entered by users and do not utilise Social Network information. The authors in [6] focus on inferring trust in Social Networks from relationships, however they also assume that the user manually assigns a rating to other users they are connected to.

The authors in [4] propose a method for asserting trust amongst users based on profile similarity. Although they provide beneficial results showing that users trust others who are more similar to them, they do not assert trust on the similarities within profiles. The authors [19] also propose a profile similarity approach. However, their work assess similarity based on similar trust decisions rather than on profile attributes as our approach.

The authors in [7] propose the "Web of Trust" in a Social Network where users give ratings to each other and based on the links amongst users, a "Web of Trust" is formed. However, they also assume that users manually assign a trust ranking to other users.

The authors in [1] provide a comprehensive study that cover policy-based trust, reputation-based trust, general models of trust and trust in information resources. Policy-based trust involves using credentials with digital signatures however none use the WebID protocol. Reputation-based trust consists of trust based on the trust opinions of other users, however all the work assumes that the users manually allocate their trust values to their opinions. General models of trust focuses on a broader view of trust mechanisms, however the authors assume that the trust values are provided. Trust in information resources examines trust values for content, however, most of the work relies on users ranking the content.

X. Conclusion and Future Work

In this work we focused on user's trust judgements to decide whether another user is trustworthy or not. We outlined several social factors that effect trust judgements and we also explained several methods on how to automatically assert subjective trust values for these social factors from information extracted from the Social Web. These subjective trust values can be described using the Trust Assertion Ontology (TAO) which can be stored for later retrieval.

[10]The aggregated trust value is not stored.

Table I
USER 1'S ASSERTED SUBJECTIVE TRUST VALUES

User ID	Identity	Profile Similarity	Relationship	Reputation	Interactions	Aggregated Value
2	1.0	0.46	0.23	0.87	0.15	0.542
3	1.0	0.32	0.13	0.67	0.10	0.444
4	1.0	0.12	0.10	0.53	0.08	0.366
5	1.0	0.72	0.32	0.34	0.03	0.558
6	1.0	0.23	0.12	0.63	0.11	0.418
7	1.0	0.31	0.08	0.28	0.02	0.338
8	1.0	0.43	0.21	0.12	0.19	0.39
9	1.0	0.35	0.36	0.34	0.08	0.426
10	1.0	0.12	0.07	0.43	0.23	0.37
11	1.0	0.56	0.19	0.82	0.02	0.518
12	1.0	0.44	0.02	0.39	0.06	0.382
13	1.0	0.73	0.08	0.64	0.12	0.514
14	1.0	0.22	0.34	0.34	0.09	0.398
15	1.0	0.45	0.11	0.32	0.08	0.392

Information confidentiality was presented that provides the user to define a trust threshold for each specific part of the user's information that needs to be satisfied in order for a requester to be granted access.

We also have extended the Privacy Preference Framework to include a Trust Manager that asserts subjective trust values and to filter information based on whether the subjective trust value is greater than the information confidentiality value.

Although the primary focus of this work was to illustrate that subjective trust values can be asserted from Social Web data, as future work, we will compare our methods to other trust assertion computations and demonstrate how this social-based trust can be useful for other scenarios. Moreover, we will also examine when to update the stored asserted trust values and we will also improve our trust assertions by automatically assert trust for relationship types.

REFERENCES

[1] D. Artz and Y. Gil. A survey of trust in computer science and the semantic web. *Web Semantics: Science, Services and Agents on the World Wide Web*, June 2007.

[2] D. Boyd and E. Hargittai. Facebook privacy settings. Who cares? *First Monday*, 15(8), August 2010.

[3] J. Golbeck. Generating predictive movie recommendations from trust in social networks. In *Trust Management*, iTrust'06, 2006.

[4] J. Golbeck. Trust and nuanced profile similarity in online social networks. *ACM Transactions on the Web*, Sept. 2009.

[5] J. Golbeck and J. Hendler. Accuracy of metrics for inferring trust and reputation in semantic web-based social networks. In *Knowledge Engineering and Knowledge Management*, EKAW'04, 2004.

[6] J. Golbeck and J. Hendler. Inferring binary trust relationships in web-based social networks. *ACM Transactions on Internet Technology*, Nov. 2006.

[7] J. Golbeck, B. Parsia, and J. Hendler. Trust networks on the semantic web. In *Cooperative Intelligent Agents*, 2003.

[8] T. Grandison and M. Sloman. A survey of trust in internet applications. *IEEE Communications Surveys and Tutorials*, 2000.

[9] O. Hartig. Querying trust in rdf data with tsparql. In *European Semantic Web Conference*, ESWC'09, 2009.

[10] S. P. Marsh. *Formalising Trust as a Computational Concept*. PhD thesis, University of Stirling, April 1994.

[11] D. Olmedilla, O. F. Rana, B. Matthews, and W. Nejdl. Security and trust issues in semantic grids. In *Semantic Grid*, 2005.

[12] F. Orlandi, J. G. Breslin, and A. Passant. Aggregated, interoperable and multi-domain user profiles for the social web. In *I-SEMANTICS '12*, 2012.

[13] O. Sacco and J. G. Breslin. PPO & PPM 2.0: Extending the privacy preference framework to provide finer-grained access control for the web of data. In *I-SEMANTICS '12*, 2012.

[14] O. Sacco and A. Passant. A Privacy Preference Manager for the Social Semantic Web. In *Semantic Personalized Information Management Workshop*, SPIM'11, 2011.

[15] O. Sacco and A. Passant. A Privacy Preference Ontology (PPO) for Linked Data. In *Linked Data on the Web Workshop*, LDOW'11, 2011.

[16] O. Sacco, A. Passant, and J. G. Breslin. User controlled privacy for filtering the web of data with a user-friendly manager. In *Poster Session at I-SEMANTICS '12*, 2012.

[17] O. Sacco, A. Passant, and S. Decker. An Access Control Framework for the Web of Data. In *IEEE TrustCom-11*, 2011.

[18] H. Story, B. Harbulot, I. Jacobi, and M. Jones. FOAF + SSL : RESTful Authentication for the Social Web. *Semantic Web Conference*, 2009.

[19] C.-N. Ziegler and J. Golbeck. Investigating interactions of trust and interest similarity. *Decision Support Systems*, Mar. 2007.