This document is published in:

Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2012, pp. 1387 - 1392.
DOI: 10.1109/TrustCom.2012.288

U+F Social Network Protocol: Achieving interoperability and reusability between Web Based Social Networks

Lorena González-Manzano
Univ. Carlos III de Madrid
Leganés, Spain
lgmanzan@inf.uc3m.es

Ana I. González-Tablas
Univ. Carlos III de Madrid
Leganés, Spain
aigonzal@inf.uc3m.es

José M. de Fuentes
Univ. Carlos III de Madrid
Leganés, Spain
jfuentes@inf.uc3m.es

Arturo Ribagorda
Univ. Carlos III de Madrid
Leganés, Spain
arturo@inf.uc3m.es

***Abstract*—Along the time many Web Based Social Networks (WBSNs) have appeared, but not all of them offer the same services. Users may use multiple WBSNs to satisfy their requirements. Besides, operations such as the creation of accounts or the establishment of groups, are repeated in all of them, being a tedious issue. To address this matter, this paper proposes a protocol, based on the UMA core protocol and the FOAF project, to attain interoperability and reusability of resources, identity data and access control policies across different WBSNs. Moreover, an evaluation and a security analysis are presented.**

KEYWORDS: INTEROPERABILITY, REUSABILITY, ACCESS CONTROL, SOCIAL NETWORKS.

I. INTRODUCTION

The World Wide Web is full of Web Based Social Networks (WBSNs) but not all WBSNs offer the same services and users have to decide which of them is more adequate to satisfy their expectations. Besides, being user of several WBSNs requires, for each of them, the creation of accounts, the establishment of contact groups, the upload of resources and the specifications of access control policies. Thus, the problem emerges: is it possible to share resources with users of different WBSNs without performing repeated operations? In other words, can interoperability and reusability between different WBSNs be attainable?.

Along the time there have been multiple attempts to provide some kind of interoperability between WBSNs, analysed in Section II. Interoperability, given a definition found in [1] and applying it to the social application context, is the ability of WBSNs to work together within and across any type of boundary in order to advance the effective communication of all users. In the literature it is called the *Walled Garden Problem* [2] and it can also be associated with the access from different WBSNs to resources, identity data and access control policies where resources correspond to photos, videos and so on and identity data refers to profile and contact relationship data. By contrast, reusability has not been particularly studied in the WBSN context. Nonetheless, reusability can be identified as a complementary feature to interoperability because if a pair of elements are interoperable between multiple WBSNs, it means that they can be analogously used and, thus, they can be reused. Moreover, none development addresses either interoperability or reusability regarding resources, identity data and access control policies. Therefore, this paper proposes a solution subdividing the problem as follows:

- Decentralization of access control policies.
- Decentralization of resource management procedures.
- Decentralization of identity data.

To reach a solution to all above mentioned problems a protocol called UMA+FOAF Social Network Protocol (U+F) is developed. It bases on User-Managed Access (UMA) [3] to addresses the first pair of problems and on the Friend-Of-A-Friend (FOAF) project [4] to satisfy the last issue. On the one hand, UMA is applied because it focuses on multiple interoperable domains but there are not UMA prototypes or works related to a concrete WBSN scenario. Moreover, UMA identity management, though being in progress [5], is not the main goal. On the other hand, as identified in [6], FOAF seems a promising approach to specify users' identity. Indeed, multiple current WBSNs, such as Facebook or Youtube, and social applications, like Second Life, make use of it.

The rest of the paper is structured as follows. Section II contains related work. Section III specifies the purpose, objectives and architecture of U+F. In Section IV the definition of identity data managed in U+F is presented. Section V presents a description of U+F phases. Section VI describes the evaluation. Finally, in Section VII conclusions and open research issues are identified.

II. RELATED WORK

Interoperability and reusability have been addressed in several proposals but none of them consider resources, identity data and access control policies, Table 1.

In respect to resources interoperability and reusability three proposals are noticed. Distributed Social Network Protocol (DSNP) [7] bases on developing a distributed social network in which users create their profiles, store them in free chosen hosts and exchange resources with their contacts through cryptographic mechanisms. From a distributed perspective, LotusNet [8] consists of a peer-to-peer system in which peers store resources locally and rely on cryptography

Table I: Related work description

	Requirements		
	G. identity data	G. access control policies	G. resources
Proposals			
DSNP [7]			√
LotusNet [8]			√
OneSocialWeb [9]			√
UMA [3]		√	√
OpenID [10]	√		
FOAF [4]	√		
Microformats [12]	√		
MyProfile [11]	√		

to guarantee strong authentication. Other relevant proposal is OneSocialWeb [9], it focuses on connecting of all WBSNs analogously to emails are managed in different platforms.

On the other hand, some proposals address identity data interoperability and reusability. Commonly, a service, referred as Identity Provider (IdP), is in charge of the storage and the delivery of user identifications. A crucial example is OpenID [10], a decentralized identification standard used to identify users through URLs. Likewise, other contribution is MyProfile [11], a single-sign-on procedure that authenticates users by combining WebID and FOAF. Slightly different is the Friend-Of-A-Friend (FOAF) project [4] which provides a machine-readable ontology to describe people, things they create and do and links between them. It combines the use of the Resource Description Framework (RDF) and the Web Ontology Language (OWL). Similarly, Microformats [12] are used to describe people, companies, organizations and places but it is not as easy and friendly as FOAF and, by now, solutions are not specifically related to social relationships.

Looking for resources and access control policies interoperability and reusability, User-Managed Access (UMA) Working Group has developed an architecture and protocol called UMA [3]. It puts the user in charge of assigning access rights to resources.

III. System overview

U+F is a novel approach to achieve interoperability and reusability between different WBSNs. Users control their resources, identity data and access control policies without requiring a specific WBSN to carry out these tasks. Resources are stored in a particular number of hosts, identity data is located in chosen IdPs and access control policies are established in selected Authorization Managers.

As identified in Figure 1,supposing a user, User1, who is a Facebook and a Badoo member, and other user, User2, who is exclusively member of MySpace, they can interact with each other because their identity data and resources are accessed through WBSNs. Furthermore, as User1 has multiple accounts, if desired, the same resources, access control policies and identity data can be used.

A. Security goals

1) WBSNs have to access to the minimum data [13]. Once a WBSN accesses to data of a WBSN user, the management has to be carried out using the least possible data.

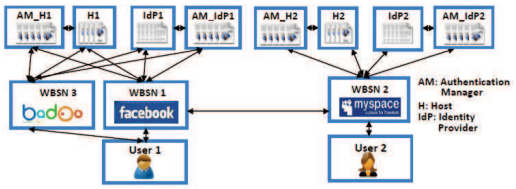

Figure 1: WBSNs - A single world

2) Requested data has to be only accessed by authorized users.
3) User impersonation must be avoided. Requested data has to be exclusively delivered from one WNSN to another, being certain about the fact that the requested WBSN does not impersonate the requesting user.

B. Architecture

U+F architecture consists of six entities, Figure 2:

User (U): a user has a pair of roles. Firstly, a user plays the role of a UMA's Requesting Party (RP) who is able to access resources of his contacts through Social Networks. Secondly, a user also plays the role of an Authorizing User (AU) by performing three main operations, the placement of resources in his Host together with later updates of them, the deployment of his FOAF file in his IdP and the deployment of policies in his Authorization Managers.

Identity provider (IdP): repository of FOAF files which are placed by AUs, as well as, provider of claims. Moreover, each IdP owns a certificate generated by an IdP Certification Authority (IdP_CA) to prove their validity and correctness in respect to other IdPs and AMs. Besides, to verify requested claims, per each user, IdPs store the list of IdP_CAs that each user considers reliable.

Host(H): repository of resources, analogous to a data base service, in which the AU establishes resources.

Authorization Manager (AM): entity that evaluates policies previously established by an AU. However, to achieve this purpose AM requests claims to perform policy validation and delivers tokens. Also, in order to verify claims, they store, per each user, the identification of trusted IdP_CAs.

Besides, it is possible the existence of multiple AMs, Hosts and IdPs which depends on users' choice but, for the sake of simplicity, it is considered one Host and one IdP per user, and one AM for each of these entities, Figures 1, 2.

Social Network (SN): WBSNs are referred as SNs. They provide an interface to show resources and identity data and facilitate the management of wall comments or other services. It takes the role of a UMA requester, acts on behalf of a RP and interacts with Hosts to reach protected resources. Also, each time a user session starts, after performing the user authentication regarding his Host and IdP, SNs interact with the adequate IdP to get user personal data.

On the other hand, each SN owns a certificate generated by a SN Certification Authority (SN_CA) and stores, per each user, the identification of the SN_CAs that each user considers reliable. Therefore, once a request is sent from a

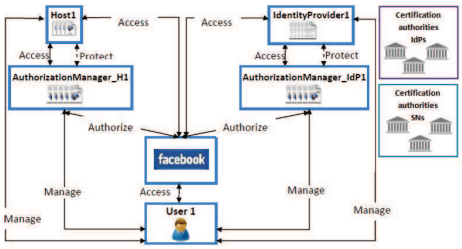

Figure 2: Architecture

SN to another, taking both the role of a requester, called herein Fat Requester, certificates authenticate both SNs.

In the connection between SNs, given that it is not specified in UMA, SSL is applied.

Certification authorities (CA): these entities are divided in two groups. A first group provides certificates to trusted IdPs (IdP_CAs) and another group to trusted SNs (SN_CAs). Certificates delivery is performed regarding specific criterion and rules whose specification is an open research issue.

The existence of groups of CAs instead of a single entity is due to the huge quantity of WBSN users and the complexity of its management. Likewise, also looking for the simplification of certificates management, there are CAs to independently certify IdPs and SNs.

Notice that trust relationships between IdPs, Host and AMs are established through the storage of above mentioned identification lists of IdP_CAs and SN_CAs.

IV. Personal file

Identity data refers to profile and contact relationship data which are structured in a FOAF file specially developed for U+F. In the FOAF project specification [14] a great set of available attributes are defined. However, some other attributes have been created in this work. Regarding profile data, it is developed the attribute ”WBSNs” which refers to the name of WBSNs, separated by a space, that the contact is registered in. Moreover, profile data consists of, at least,the user name and the user email address which, for security reasons, is stored after having applied a hash function to it. On the other hand, in respect to relationship data, the following attributes per relationship have been developed: ”creation date”, that refers to the date when the relationship was established; ”trust”, that corresponds to a numeric relationship trust level (1-the least; 10-the most trusted); ”duration”, which corresponds to the relationship validity period; and ”WBSNs” analogous to the one aforementioned. Moreover, in respect to relationships, they are unidirectional and supposing that a user, called Bob, has a work relationship with a user called Alice, his FOAF file includes Alice’s relationship but not necessarily in the other way round.

Nonetheless, in U+F reduced FOAF files are also used. In general, they correspond to a FOAF file without relationship information and with attributes regarding access control policies.

V. U+F protocol description

A. Initialization

The initialization, subdivided in three steps, focuses on preparing entities with all required information.

1) Registration of entities: It involves the registration of a Host at an AM and the registration of an IdP at an AM, which can be the same AM or a different one. These registrations are equivalent to the introduction of a Host to an AM described in UMA [15]. A user, in the role of an AU, introduces the Host or the IdP in the chosen AM to make available later validation of tokens.

To conclude, registration finishes when the user specifies in his AMs and IdPs the list of trusted IdP_CAs.

2) Registration of resources and identity data: This phase focuses on registering new resources and the appropriate FOAF file in the selected Host and IdP. Specifically, the registration of resources and identity data is equivalent to UMA [15]. Once again each user takes the role of an AU.

3) Specification of main information in WBSNs: In each WBSN, once a user logins for the first time, he specifies the IdP in which his FOAF file is stored and the Host which stores his resources. Besides, to achieve interaction between WBSNs, each user specifies the list of SN_CAs in which each of them trusts.

B. User logins in a WBSN

Each time a user logins in a WBSN, taking the role of a RP, his profile and contacts are directly presented and his resources remain accessible. To acquire these data, the user is authenticated against his IdP and Host by the SN and, then, each SN, in the role of a requester and on behalf of the user, contacts to the user’s IdP and Host to get his FOAF file and resources respectively. The step of accessing a protected resource of UMA protocol [15] is executed twice, one to get the FOAF file and another to acquire resources.

The process requires the acquisition of claims and the necessary mutual authentication between the RP and his Host and IdP to later delegate access to SNs, being these issues not detailed in UMA. Authentication can be carried out applying multiple mechanisms and protocols. Using symmetric cryptography, some mechanisms in respect to the Challenge-Response protocol are a feasible choice. By contrast, though increasing complexity, public key cryptography is another alternative, for example the mechanism proposed by [16]. However, avoiding impersonations requires authenticate the user in the WBSN log in and out. Furthermore, also trying to prevent this issue, all performed signatures include a time stamp. Thus, users in access control policies specify an accepted time stamp threshold. Also, note that time is obtained by a trusted site like NIST Internet Time Service.

In relation to claims, AM_IdP requests claims to provide the appropriate token regarding the requested FOAF file and they correspond to a proof of the identity of the owner of the

requested file, the RP. On the other hand, AM_Host requests claims to provide a token to access requested resources and they also correspond to a proof to identify the RP. In order to acquire claims, the SN in which the RP delegates requests the accreditation of the RP to the IdP. Then, the IdP creates a signed structure, including a reduced FOAF file with the name and email of the user, which corresponds to claims. Finally, when AMs receive claims, they verify signatures, making use of the list of IdP_CAs specified by the user, and validate access control policies to later deliver tokens. Once claims and tokens are obtained, they are stored in the SN for the whole session of the user. Then, if needed, they are delivered without having to be requested again. Nonetheless, the erasure of tokens and claims when a user logs out is recommendable to prevent unnoticed impersonations.

According to Figure 3, the technical specification of the most relevant message, being equivalent the FOAF file and resource acquisition, is the following:

6) User1 accreditation: the IdP sends a signed reduced FOAF file which includes the name and email of the RP and a time stamp. For example, it is supposed that a user, Bob, logins in a SN.

<rdf:RDF> ... <foaf:Person rdf:nodeID="RequesterBob" > <foaf:name>Bob Smith Brown </foaf:name> <foaf:mbox_sha1sum>8567c8b121ffcd99604a40jhf5 52a2d884c234b3 </foaf:mbox_sha1sum> </foaf:Person> </rdf:RDF> + timeStamp + **Signature of IdP_Bob**

C. User accesses to a contact's data

Once a user is within a WBSN in multiple circumstances desires to access to data of his contacts. However, if contacts are enrolled in different WBSNs, interactions between these applications are indispensable. First of all, given a user of SN1, User1, who wants to access to resources of one of his contacts, User2, all WBSNs in which User2 is registered in have to be identified. Indeed, this information is available in the FOAF file of User1, as described in Section IV. Then, User1 chooses one WBSN, for example SN2, and the procedure described in this Section is performed.

When User1 desires to visualize the profile and resources of User2, he clicks on User2 relationship, and if this user also has a relationship with User1, the profile and resources are delivered according to User2's access control policies.

This process is composed of a pair of UMA protocol executions in respect to the step of accessing a protected resource. One execution is carried out to acquire the reduced FOAF file of User2. The second UMA execution corresponds to the acquisition of resources of User2 and it can be performed repetitively.

For the sake of simplicity and due to the analogy between acquiring the profile and resource of User2, which only differs on requesting data to an IdP or to a Host, in the following Section, the acquisition of the FOAF file is described and it is depicted in Figure 4.

1) FOAF file acquisition: The procedure differs from UMA in a couple of points. On the one hand, SN1 and SN2 play the role of a Fat Requester (pointed out in Section 2).

On the other hand, claims are clearly detailed. In particular, to obtain the token that grants access to requested identity data, the AM_IdP_User2 requests claims to User1 that consist of three elements. The first element corresponds to a proof of his relationship with User2. Considering that relationships are unidirectional, this proof refers to a relationship structure regarding the existence of User1 relationship in the FOAF file of User2. The second element corresponds to a proof of possessing some attributes. This proof is a structure that depends on access control policies, thereby attributes can be requested or not and they can differ from one request to another. The last proof corresponds to the identification of the RP, User1.

More specifically, in order to get claims, User1 can provide them or delegate in SN1. Supposing that User1 delegates in SN1, this SN acquires, through IdP_User1, a signed structure in relation to requested attributes, a signed structure to certify User1's identity and a signed relationship structure which identifies the relationship between both users. After obtaining the last pair of structures, they are sent to SN2 and redirected to IdP_User2. Then, when IdP_User2 verifies the received signed structures and if the requested relationship exists, it signs the received relationship structure and sends it back to SN1. Lastly, SN1 sends claims to AM_IdP_User2.

The technical specification of relevant messages regarding this procedure is described above. All presented messages correspond to an example in which a User1, called Bob, wishes to access the profile data of a User2, called Alice. Moreover, to access to Alice's data, Bob has to be student of Carlos III University and older than 20.

8) User1/SN1 claims request(User1-User2 relationship authentication+User1 needed data): AM_Host_User2 requires as claims a relationship structure to verify the relationship between the RP and the owner of the data, and an attribute structure to verify access control policies, being both of them composed of two parts.
The relationship structure consists of a pair of tags. On the one hand, between the tags <first> and </first>, it is included a reduced FOAF file with the name and email of User1. On the other hand, between the tags <end> and </end>, it is included a reduced FOAF file with the name and email of the user whose resources want to be accessed, User2.
The attribute structure consists of a couple of tags. On the one hand, between tags <attributes> and </attributes> attributes to perform policy validation are included. On the other hand, between tags <attributesData> and </attributesData> a reduced FOAF file with the name, email and requested attributes of the RP is included.
In the example, chief issues to determine are the verification of the relationship between Alice and Bob and Bob's possession of requested attributes.

<**first**> </**first**> <**end**> </**end**> + <**attributes**>schoolhomepage age</**attributes**>
<**attributesData**></**attributesData**>

11) Signed(User1 accreditation)+Signed(User1-User2 relationship)+Signed(User1 needed data): IdP_User1 sends a signed reduced FOAF file which includes the name and email of the User1, a signed relationship structure identifying the relationship that has to be certified and a signed attribute structure which includes a reduced FOAF file with attributes requested, all of them associated with a time stamp. In the example Bob receives an accreditation of his identity, the relationship structure specifying that he wants to access to Alice data and an attribute structure which certifies the possession of requested attributes.

<rdf:RDF> ... <foaf:Person rdf:nodeID=" RequesterBob" > <foaf:name>Bob Smith Brown</foaf:name> <foaf:mbox_sha1sum>8567c8b121ffcd99604a40jhf5 52a2d884c234b3 </foaf:mbox_sha1sum> </foaf:Person> </rdf:RDF> + timeStamp + **Signature of IdP_Bob**
<**first**> <rdf:RDF> ... <foaf:Person rdf:nodeID=" RequesterBob" > <foaf:name>Bob Smith Brown </foaf:name> <foaf:mbox_sha1sum>8567c8b121ffcd99604a40jhf5 52a2d884c234b3 </foaf:mbox_sha1sum> </foaf:Person> </rdf:RDF> </**first**> <**end**>
<rdf:RDF> ... <foaf:Person rdf:nodeID=RequesterAlice> <foaf:name>Alice Cook Adams </foaf:name> <foaf:mbox_sha1sum>8567c8b121ffcd99604a40jhf552 a2d884c234b3 </foaf:mbox_sha1sum> </foaf:Person> </rdf:RDF> </**end**>+ timeStamp + **Signature of** IdP_Alice+ <**attributes**>schoolhomepage age</**attributes**> <**attributesData**> <rdf:RDF> ... <foaf:Person rdf:nodeID=" RequesterBob" > <foaf:name>Bob Smith Brown</foaf:name> <foaf:mbox_sha1sum>8567c8b121ffcd99604a40jhf5 52a2d884c234b3</foaf:mbox_sha1sum> <foaf:schoolhomepage> www.uc3m.es</foaf:schoolhomepage> <foaf:age>26</foaf:age> </foaf:Person> </rdf:RDF> </**attributesData**>+ timeStamp + **Signature of IdP_Bob**

15) Signed(User1-User2 relationship): IdP_User2 signs the relationship structure received (removing the previous signature) if User1 is in the FOAF file of User2, thereby guaranteeing a relationship between them.

In conclusion, there are some points to highlight. Firstly, in case multiple data are joined under the same policy, the token obtained provides access to all of them. Secondly, as pointed out in Section V-B, claims are stored in the SN that initially sends the request to, if required, be later delivered without being requested again. Similarly, tokens achieved are stored and reused if their expiration time does not exceed.

VI. Evaluation

A. Interoperability and reusability

Data used in U+F is decentralized, resources are stored in Hosts, identity data in IdPs and access control policies in AMs. Then, data can be replaced, moved or updated without affecting any service of WBSNs. Also, given the decentralization, different WBSNs can make use of the same resources, identity data and access control policies when the same IdPs and Host are linked to them.

Regarding interoperability, as described along the whole paper, the use of the same identity data specification, FOAF files in this case, and the use of a concrete application of UMA, including the specification of claims and the Fat Requester, address this issue.

B. Performance

Trying to attain more specific results, Table 2 presents per each protocol phase and according to Figure 3 and Figure 4 (considering contact resource acquisition too), the number of messages exchanged, the number of entities involved, the computational cost in relation to performed operations over data stored in IdPs and Hosts and the total complete executions of phases of UMA protocol. Nonetheless, in order to have a general perception of U+F executions, phases *User logins in a SN* and *User accesses to a contact's data* are studied regarding the worst and best case. In relation to the worst case, it is assumed that all messages of the protocol are carried out because no information is stored and reused. On the contrary, according to the best case, it is assumed that claims and tokens are stored and reused.

Table II: U+F evaluation

U+F phases	No. Messages	No. Entities	Computational Cost	UMA Executions
Registration of entities	10N+10M	N+M+1	O(1)	N
Registration of resources and identity data	$3(P_X+I_X)$	N+M+T+1	O(1)	P_X
		Worst case		
User logins in a SN	$11+11R_X$	5	$O(Z_X)+O(P_X)$	$1+R_X$
User accesses to contact data	$23+23R_2$	7	$O(Z_2)+O(Z_1)+O(P_2)$	$1+R_X$
		Best case		
User logins in a SN	$11+5R_X$	3	$O(Z_X)+O(P_X)$	1+1
User accesses to contact data	$23+9R_2$	4	$O(Z_2)+O(Z_1)+O(P_2)$	1+1

N = No. registered Hosts by a user
M = No. registered IdPs by a user
T = No. registered AMs by a user
R_X = No. Resources accessed in the Host of UserX
Z_X = No. FOAF files stored in the IdP of UserX
P_X = No. Resources stored in the Host of UserX
I_X = No. Identity data stored in the IdP of UserX

From Table 2 some relevant features can be inferred. Regarding the number of messages exchanged, it is significant the quantity of them required in the registration phase, which increases in respect to the number of entities involved. Similarly, though equivalent to current WBSNs, the number of messages in the registration of resources increases in relation to the number of registered resources. However, the most significant exchange of messages corresponds to *User logins in a SN* and *User accesses to a contact's data*. Both phases involve a great quantity of messages but claims and tokens are usually reused and, as shown in the best case, the number of messages can be significantly lower.

In respect to entities, the use of multiple AMs, Hosts and IdPs is specially significant in registration processes. Nonetheless, it is not expected the used of a huge quantity of these entities. For example, one IdP per user is expected.

On the other hand, according to computational cost, it is remarkable the complexity of *User accesses to a contact's data* which, despite being linear, is the highest one and depends on multiple variables.

Lastly, in respect to UMA executions, the difference between the worst and best case is extremely noticeable and understandable. If tokens expiration time exceeds, they are reused and complete executions of UMA are avoided.

C. Security analysis

This Section analyses the satisfaction of the security goals highlighted in Section III.

The acquisition of claims can be carried out in multiple ways. For example, exchanging complete FOAF files between WBSNs. Nevertheless, to satisfy the first of security goals, which refers to the fact that WBSNs access to the minimum data of other WBSNs contacts, data exchanged is limited to name, email and WBSNs in which each user is enrolled in. In the worst case if users establish "public" access control policies, WBSNs get access to all users data. By contrast, in a better case, if users restrict access

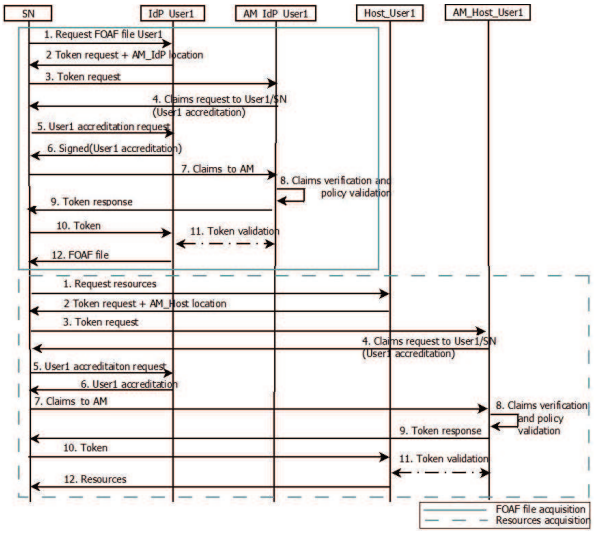

Figure 3: User logins in a SN

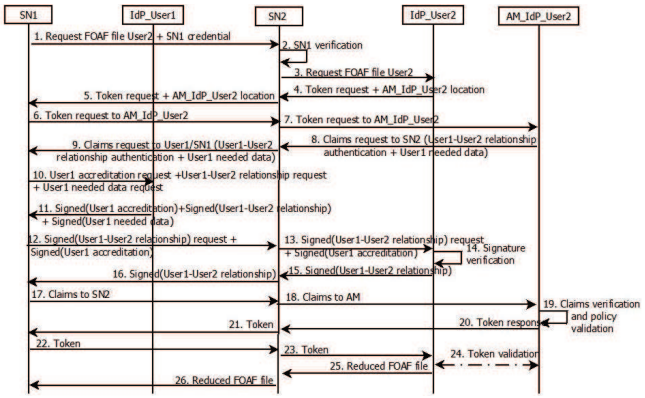

Figure 4: User accesses a to contact FOAF file

to personal attributes such as their hobbies, the procedure developed prevents WBSNs from knowing them.

On the other hand, data confidentiality is achieved by the establishment of access control policies attached to data.

Finally, user impersonation is mainly avoided due to the mutual authentication between each user and his IdP and Host, in the log in and out in a WBSN. Then, the user's IdP and Host are informed about his presence in the application. Moreover, signatures that include a time stamp and the consideration of trusted relationships between IdPs, Hosts and AMs through the storage of identification lists of IdP_CAs and SN_CAs are also essential to address this issue.

VII. Conclusions and Open research issues

Many WBSNs are currently in use and given their lack of interoperability and reusability, this work proposes a solution called U+F Social Network Protocol that bases on the UMA protocol and the FOAF project.

This proposal can be extended in several ways. First, users are not completely in control of their data and once presented to WBSNs, these applications can take over them. A possible solution focuses on the use of cryptography. Second, the inclusion of complex access control policies regarding multiple jumps is an open research issue. Third, other open issue refers to the inclusion of OpenID in U+F, simplifying the management of users identification. Finally, highlighted in Section III-B, constraints and rules to specify the validity of trusted IdPs and AMs have to be detailed.

References

[1] H. Directors. (2005) Interoperability definition and background. [Online]. Available: http://www.himss.org/content/files/interoperability_definition_background_060905.pdf

[2] C. man Au Yeung, I. Liccardi, K. Lu, O. Seneviratne, and T. Berners−Lee, "Decentralization: The future of online social networking," in *W3C Wks. on the Future of Social Networking Position Papers*, 2009.

[3] (2009) Kantara initiative. [Online]. Available: http://kantarainitiative.org/

[4] The friend of a friend (foaf) project. [Online]. Available: http://www.foaf−project.org/

[5] (2010) Uma faq: How is uma related to openid and openid connect? [Online]. Available: http://kantarainitiative.org/confluence/display/uma/UMAFAQ

[6] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "A semantic web based framework for social network access control," ser. SACMAT '09. ACM, 2009, pp. 177–186.

[7] Dsnp: Distributed social networking protocol. [Online]. Available: http://www.complang.org/dsnp/

[8] L. M. Aiello and G. Ruffo, "Lotusnet: Tunable privacy for distributed online social network services," *Comput. Commun.*, vol. 35, pp. 75–88, 2012.

[9] (2011) Onesocialweb. [Online]. Available: http://onesocialweb.org/index.html

[10] (2011) Openid. [Online]. Available: http://openid.net/

[11] A. Sambra and M. Laurent, *MyProfile Decentralized User Profile and Identity on the Web*, 2011.

[12] Microformats. [Online]. Available: http://microformats.org/

[13] A. Kung, J. Freytag, and F. Kargl, "Privacy-by-design in its applications : The way forward," in *D-SPAN*. IEEE, 2011.

[14] Foaf vocabulary specification. [Online]. Available: http://xmlns.com/foaf/spec/#term_workplaceHomepage

[15] M. P. Machulak, E. L. Maler, and D. Catalano, "User−Managed Access to Web Resources," *Security*, pp. 35–44, 2010.

[16] C. C. Security, U. S. D. O. Commerce, and S. W. Director, "Entity authentication using public key cryptography," 1997.