On the Application of Trust and Reputation Management and User-centric Techniques for Identity Management Systems

Ginés Dólera Tormo
Security Group
NEC Laboratories Europe
Email: gines.dolera@neclab.eu

Félix Gómez Mármol
Security Group
NEC Laboratories Europe
Email: felix.gomez-marmol@neclab.eu

Gregorio Martínez Pérez
Department of Information
and Communications Engineering
University of Murcia
Email: gregorio@um.es

***Abstract*—Identity management systems have been designed to deal with the authentication and authorization process. They enable Single Sign-On, where a user can make use of an unique account to access different services, and preserve users' privacy, maintaining users' attributes on reliable providers. However, current identity management systems still lack in giving control to the users to decide which personal information could be released to a given service. In the same way, they do not inform the users about how their personal information will be dealt once released. In this document we present how trust and reputation management and user-centric techniques can be combined with identity management systems to solve these challenges.**

I. INTRODUCTION

In the last years, due to the great success of information systems, users exchange information more and more, including private information and personal data. However, these users are rarely aware of how their personal data is being managed, and they do not know who are really allowed to get this information. Additionally, users have to deal with registration procedures each time they want to access a service from a service provider with which they have not interacted before. This registration procedures requests information about the users, which is not necessary to the provision of the service itself in most of the cases.

Having information about users is increasingly considered valuable, even it becomes a target to some organizations for business interests, especially for advertising purposes. It is also aimed to develop advanced attacks on specific targets based on information collected from them. In general, organizations try to collect users' information through registration forms. Users are required to create a new account for each service they want to use, for instance they need to perform a registration process just to write some comments in a blog.

Registration forms usually request users personal information, such as email address or birth date. Moreover, some registration processes collect other private data, which is not actually needed for the provision of the service itself, such as telephone number, hobbies, real name, etc. Dealing with this process not only results in having to remember different usernames and passwords for each service and be subject of receiving spam, but also it threatens users' privacy. For example, users do not usually know if their private information will be used in marketing campaign belonging outside to the service provider they are accessing.

Privacy, and more specifically, having control over the information that other entities can have about oneself, are desired features by users of any communication system. Additionally, these topics are being considered in certain geopolitic environments, such as the European Union, as a right of the users [11]. In this context we find those users who do not want to link their private lives with their interactions in different websites they visit, or those who do not want that information about their preferences and usage profiles to be collected. For instance, reporters who want to denounce situations without being concerned about possible retaliation, soldiers who cannot or should not disclose their geographic location, or simply as a measure of safety for any user of communications over the Internet.

With these assumptions identity management systems (IdM) began to emerge a few years ago, suggesting an alternative to these registration processes. Through establishing trust relationships between different providers, end users are able to store their attributes in reliable entities, which are in charge of preserving users' privacy. However, current identity management systems do not give enough control or information to the users for managing their private information.

In this document we identify some of the main challenges that current identity management systems should deal with regard to the management capabilities and information that users have about their personal attributes. Our contribution in this document is to describe how trust and reputation management and user-centric techniques can be integrated into identity management systems in order to solve the described challenges.

II. BACKGROUND

Identity management systems were designed with the aim of providing an access control architecture, able to preserve users' privacy and enabling Single Sign-On by establishing trust relationships between different organizations.

Shibboleth [1] and Liberty Alliance [2] are widely extended examples of identity management systems. In these systems, users' information is stored on reliable entities, such as their city council or university, named identity providers. Identity providers are in charge of managing users' identities, releasing just needed information to external entities as shown in Figure 1. Indeed, service providers delegate the authentication process to these identity providers, which in turn send required users' information after a successful authentication.

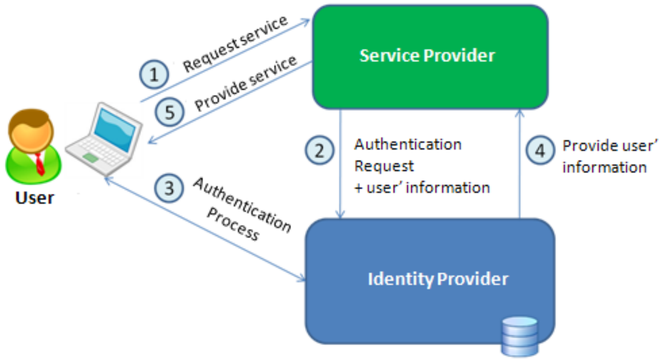

Fig. 1. Overview of an Identity Management System

Since they make use of pseudonyms, identifiable information or attributes, such as email address or real name, do not have to be disclosed if they are not actually required. Additionally, they enable Single Sign-On, allowing users to access different services using their unique account. From the access control point of view, this solution also allows service providers to define who is allowed to access a specific service through access control policies.

However, these systems do not give enough control to the users for managing their information. Once authenticated they cannot decide which attributes should or should not be released. Similarly, these systems do not give accurate information to the users about how their information will be managed once released.

OpenID [3] is defined as a user-centric identity management system. Its functionality is similar to those previously presented in the sense that users' attributes are stored in OpenID Providers (i.e. identity providers) and requested by Relying Parties (i.e. service providers), when users want to access a service given by a Relying Party. However, with regard to user capabilities, the main difference between the presented identity management systems is that OpenID Providers ask for explicit user consent before releasing any kind of personal information.

In these traditional identity management solutions, the identity providers are in charge of maintaining users' attributes and credentials. However, other approaches transfer this functionality to be maintained by the users. That is, for instance, the case of solutions which make use of Information Cards (I-cards) [4], aimed to represent personal digital identities. The concept tries to simulate real identity cards which people carry in their pockets, such as national identification card, driver license, public library member card, etc.

These cards may also contains users' attributes, which can be signed by entities (e.g. identity providers) to prove the validity of them. Nevertheless, Information card could release more attributes than required. Take, for instance, a service provider which requires users' postal address to access a service. In such a case, a user could present her national id card, but this card could also contain other non-required information, such as real name or national identification number.

Additionally, these solutions do not show if the users can trust in the entity requesting such information, nor how this information will be managed before interacting with the entity. Furthermore, the users cannot know if the requested service will fulfill the expectations of the user. Indeed, the users would like to know a priori whether the resources will be actually provided in the end and, above all, the extent to which they will suit the users' expectations [8].

Some approaches assign dynamically to each entity a trust rating, that is, a reputation based on the entity's previous performance. For some years now, trust and reputation management has emerged as a very promising and appealing trend to deal and cope with a number of security threats risking the wide use and deployment of the so-called information and communication technologies.

Thus for instance, very popular sites such as Amazon or eBay have been using this powerful tool since their early conception in order to provider their customers with very valuable information regarding the expected behavior (i.e., reputation) of the participants in their respective systems (sellers, buyers, service providers, etc.).

Due to its numerous benefits, it has been effectively applied in a multitude of scenarios or environments [9], raging from P2P networks, wireless sensor networks, vehicular ad-hoc networks, intrusion detection networks, social networks, internet of things, cloud computing, e-Commerce, etc.

III. Current Challenges in Identity Management Systems

As presented in previous section, current identity management systems still present numerous shortcomings, particularly in regards to the control that users have over their own information. Additionally, these systems also lack in giving information to the users about the different entities which finally receive users' private information. In the following we present a set of identified challenges that this kind of systems needs to address.

- **Let user select data to be released**: The service providers usually require users' attributes either for the provision of the service (e.g. in case they need the postal address to deliver something purchased), to give a customized service (e.g. their country to show specific currency), or to perform access control. As previously commented, these attributes are automatically obtained from the identity providers once the user has been authenticated. However, traditional identity management systems rarely allow users to decide which piece of personal information (or attributes) can or cannot be released to specific entities. Some solutions allow defining which attributes should or should not be released through attribute release policies, although users should manually define complex rules beforehand.

- **Dynamic attribute aggregation**: In order for the users to avoid registration processes each time they access a different service provider, they could make use of their identity providers to retrieve the required attributes. However, users could belong to different identity providers at the same time. For instance, academic information of a given user could be managed by the identity provider of her university, while information about her postal address could be managed by the identity provider of her city hall and their credit card information managed by the identity provider of her bank. In such cases, users have to choose which identity provider to use in order to provide their attributes when requested by a service. This selection depends on the requested attributes, which suppose that users need to have advanced knowledge about how their attributes are spread among the different identity providers. Furthermore, in common identity management systems it is difficult to provide attributes from different identity providers at the same time. For example, if the user needs to provide her credit card number and her postal address at once to access a service.
- **Inform the user about the entity she will interact with**: Identity management systems are based on trust relationships between entities. That implies that the identity providers should have established certain agreement with a given service provider before being able to perform any interaction with it. However, identity providers do not give any information to the users about the service provider. Therefore, users cannot know how the given service provider behaves before interacting with it, that is, if the service provider will provide the expected service. Furthermore, users cannot know if a service provider is trustworthy enough to get their attributes. For example, a user accesses a digital library service provider to buy some books, using its identity provider for authentication. The digital library service provider requests the user credit card information, which could be provided through the identity provider as well. However the user cannot know beforehand if the quality of the books is the one expected or even if it is safe for the user to give her credit card information to such a service provider.
- **Hide the accessed services from the identity provider**: Current identity management systems preserve users' privacy, concealing the real identity of the users from service providers by making use of pseudonyms. When a user accesses a service provider, she presents a signed assertion or a token stating that she has been authenticated by its identity provider, without revealing more personal information. However, since the identity provider has to create these assertions for each service, it can trace users interactions. That is, the identity provider can know which services each of its users has access to.
- **Prevent spoofing and impersonation**: In common identity management scenarios, service providers redirect the users to their identity providers in order to delegate the authentication process, also enabling Single Sign-On. This should result in having a secure authentication mechanism, since users should just remember the credentials for a unique account. In other words, if users just have to remember one password it may be a complex and secure one. However, this scenario introduces spoofing since the service provider could redirect the user to a false identity provider, simulating the appearance of the original one, with the aim of collecting users' passwords. Furthermore, if the password of a user is stolen, the malicious entity could both get all the information of the user accessing to her identity provider and impersonate the user accessing other services, since it knows the unique password of the user.
- **Trust relationships in dynamic environments**: As previously commented, identity management systems are based on trust relationships between entities. That is, a service provider accepts authentication assertions from a given identity provider since they trust each other. These trust relationships should be established beforehand based on static agreements, such as SLA (Service Level Agreement). However, in environments where entities are more dynamic, such as in a federation context, and hence the trust relationships are not easy to establish, identity management systems are hard to apply.

Even though these issues have been taken into consideration, they have not been deeply considered in the design process of such solutions. Instead, they have been considered as additional features to improve the behavior of such solutions. Current identity management systems have given higher priority to the fact of having more control over the users, through applying access control policies, i.e. deploying mechanisms able to incriminate the users if they perform malicious actions. Nevertheless, current systems have not adequately given control capabilities to the users, with regard to the capabilities of controlling how their information will be managed.

IV. Application of Trust and Reputation Management and User-centric techniques for Identity Management

In this section, it is described how trust and reputation management and user-centric techniques could be adapted and applied to identity management solutions in order to tackle the presented challenges.

A. Trust and Reputation Management

Trust and reputation management constitutes a very helpful instrument to identify malicious or selfish elements interacting in certain systems. As a research topic, it has captured the attention of both industry and Academia, leading to a torrent of

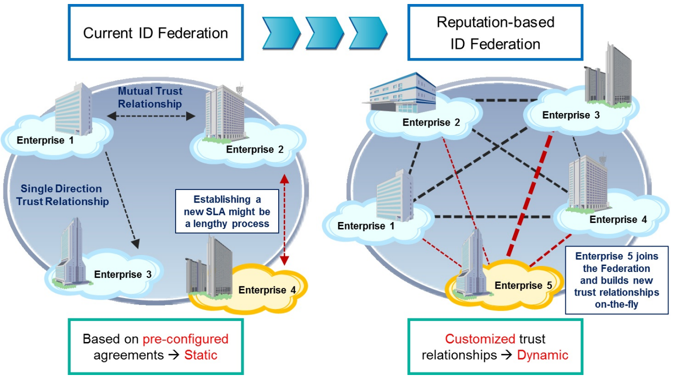
Current ID Federation
Reputation-based ID Federation
Mutual Trust Relationship
Enterprise 1
Enterprise 2
Single Direction Trust Relationship
Establishing a new SLA might be a lengthy process
Enterprise 3
Enterprise 4
Enterprise 2
Enterprise 3
Enterprise 1
Enterprise 4
Enterprise 5
Enterprise 5 joins the Federation and builds new trust relationships on-the-fly
Based on pre-configured agreements → Static
Customized trust relationships → Dynamic

Fig. 2. Reputation-based identity federation

outstanding results materialized in the form of final products, patents, standards and research articles, amongst others.

Indeed, trust and reputation management finds one of its best coupling when it is employed in conjunction with identity management systems. It is in this case where it helps IdM systems to really thrive and move to a next step, fostering in addition their wide social acceptance.

Linking with the challenges presented in section III, trust and reputation management probably represents the most suitable tool to tackle both the disinformation of the users regarding the entities they interact with, as well as the smart establishment of dynamic trust relationships.

To handle the first aforementioned challenge, trust and reputation management systems take care of gathering behavioral information about the target entity (or entities). In most cases such collected information is expressed as recommendations or feedbacks from those users who previously interacted with the target entity. Next, trust and reputation management systems perform an aggregation of such information (or an update of previous data) aiming to obtain an accurate and representative trust and/or reputation score for the target entity. Finally, such information is given to the user, who will be empowered now to make a smarter and safer decision on whether to interact or not with the target entity.

A good example of this advantageous integration was presented in a previous work [10], where an enhancement of the OpenID protocol by means of an accurate and robust trust and reputation management system was described. In this solution, users are informed about how trustworthy a relying party is, before interacting with it, in order to help users to decide if the transaction may continue.

On the other hand, the problem of those rigid systems where the establishment of new trust relationships might become a lengthy, hard and even costly issue can be very nicely addressed as well by an efficient trust and reputation management mechanism. This is the case, to name one, of the identity federation scenarios, where several entities collaborate in order to share the users' identity information they handle, for the sake of the whole community.

Nevertheless, trust relationships in these environments have been traditionally based on rigid and most of the times inflexible agreements like SLAs, hindering this way the rapid and dynamic creation, evolution and termination of identity federation systems.

Once again, trust and reputation management brings an elegant solution to this matter, as shown in Figure 2. Here, a new entity willing to enter the federation or become one of its members has the chance to do it in a seamless and dynamic fashion, without the need to trigger a lengthy negotiation process oriented to the acquisition of a SLA. To this end, each of the current members of the federation will assess the trustworthiness of the newcomer and establish new trust relationships on-the-fly, accordingly.

Moreover, those dynamically established links might evolve throughout time based on the behavior (and therefore the associated reputation score) of the new entity, meaning that the other members will exchange more or less information (users' identity attributes) with such entity according to its goodness.

B. User-centric Identity Management techniques

User-centric techniques refer to those which give extensive attention to the users in the design of a solution. Within the context of identity management, user-centric techniques have been proposed in order to give more control to the users about how their information is dealt, while at the same time being compatible with traditional identity management systems. Furthermore, since these user-centric techniques are focused on the users, they also need to have certain level of usability.

Take, for instance, these identity providers which make use of strong authentication mechanism, such as authentication based on digital certificates, to prevent spoofing or impersonation. Since the browser checks the certificate of the site to perform this kind of authentication, a user would easily realize whether her identity provider has been faked by a malicious entity. Moreover, even in case the user is maliciously authenticated, impersonation could not be possible since the user's private key is not released. Nevertheless, even though this mechanism fulfill once of the identified challenges, it usually requires more comprehensibility from the user point of view. Therefore, it is difficult to adapt in environments where technical abilities cannot be supposed from the users.

As alternative to this kind of authentication, some solutions use Information cards. As previously commented, Information cards enable users to organize their digital identities. In this sense, users could choose any card to present when they are accessing a service. Furthermore, users do not have to access their identity provider to authenticate and get their attributes each time they need to access a service.

However, Information-cards are maintained by the users, raising similar usability threats to those related to digital certificates management. Since users need additional tools managing their identities, the Identity Selector [7] has been defined to assist them in this process. This tool is in charge of storing, managing and presenting the information of the Information-cards to the user.

The Identity Selector could be an application in the user device, able to manage the different Information-cards of the user locally, or it could be used as an external service where the user accesses, in a secure way, to get one of their identity card when required. Figure 3 shows an overview of an identity management scenario where a user makes use of an Identity Selector to present required attributes.

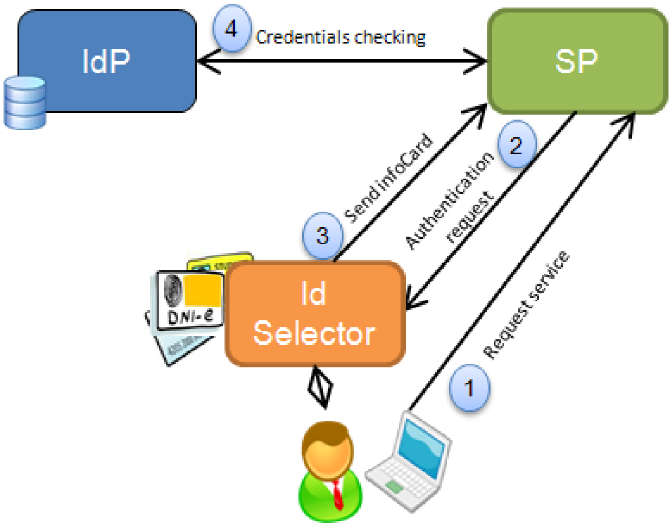

Fig. 3. Overview of a Identity Selector in a identity management system

The Identity Selector also assists users in the selection of cards. According to the attributes that are being requested, this tool is able to recommend the card to make use of. On the other hand, an Information-card could release more attributes than required, as previously commented. Furthermore, a user cannot present attributes belonging to different entities at the same time, that is, stored in different Information-card.

To tackle this dynamic attribute aggregation, some research has been done proposing solutions where an identity card is generated from attributes of other identity cards. The Higgins project [5] have designed and implemented some Identity Selectors going in this direction which could be applied to fulfill this dynamic attribute aggregation challenge.

Yet, this approach still needs to hide the accessed services from the identity provider. After sending the appropriated card to the service provider, the latter has to verify the attributes by requesting validation to the identity provider. Hence, the identity provider could trace the services that each of its user is accessing.

In order to avoid this privacy issue, this Identity Selector model could be merged with zero-knowledge proof techniques, such as U-prove [6], where users could generate claims containing just the set of attributes which have been requested. In this way, attributes presented by users are signed in such a way that the service provider could verify them without requesting validation to the identity provider.

Challenge	User-centric Techniques	Trust and Reputation Management
Let user select data to be released	Allow selecting user attributes before releasing from the identity provider (e.g. OpenID), select a specific identity (I-Cards) or select a set of attributes (U-Prove)	Non-Applicable
Dynamic attribute aggregation	Some solutions allow collecting attributed from different sources before releasing them (Higgins)	Non-Applicable
Inform the user about the entity she will interact with	Not available in current solutions	Collect recommendations about a given service provider, based on past interactions in order to inform the user about the service before accessing it
Hide the accessed services from the identity provider	Some user-centric systems do not require the users to have interactions with the identity provider to access a service provider. Instead, the attributes could be stored in the user device and directly validated by the service provider (e.g. U-Prove)	Non-applicable
Prevent spoofing and impersonation	Information-cards, among others, propose an alternative to passwords preventing spoofing and impersonation. Users do not need to send their passwords through the network nor introduce them in an external website	Trust and reputation systems avoid malicious entities, since they are punished if they are not behaving properly. Users do not accept services of malicious service provider since they get low reputation
Trust relationships in dynamic environments	Require trust relationships previously established	Trust relationships could be established dynamically since they could be based on past interactions

TABLE I
ANALYSIS OF CHALLENGES REGARDING USER-CENTRIC TECHNIQUES AND TRUST AND REPUTATION MANAGEMENT

V. CHALLENGES ANALYSIS

In section IV-B we have described how user-centric techniques could resolve some of the challenges presented by current identity management systems regarding to the control given to the users about their private information. These techniques tend to give more selection capabilities to the users in such a way that they can choose which digital identity they want to present to a specific service. One of the main aim of these techniques is also preserve users' privacy, since they are able to release just the needed private information to access a service.

Similarly, section IV-A describes how trust and reputation management systems could resolve some of the challenges regarding the information given to the users about the services they are accessing to. Before releasing private information to a given service provider, these systems collects recommendations from other users or entities about such a service provider. These recommendations are based on past experiences and they could predict, to some extend, the behavior of the service provider. According to the recommendations, the users can have an idea of the expected service and if they can trust in the service provider. Finally, they could decide if they want to continue (or not) the communication with the service provider, and hence releasing the requested attributes.

In general, even though user-centric techniques allow users to control which information each entity could have, they do not show if the users can trust in the entity requesting such information, nor how it will be managed. Furthermore, the users cannot know if the requested service will fulfill the expectations of the user. However, the integration of both user-centric techniques and trust and reputation management, within identity management context, could result in improved identity management systems able to give more control and information to the users. Table I summarizes how the combination of both topics would achieve the described challenges.

VI. Conclusion

Identity management systems have been designed with the aim of enabling Single Sign-On and preserving users' privacy. Nevertheless, current identity management systems still present some challenges to be solved, with regard to the management capabilities that the users have about their personal attribute. In the same way, users are not properly informed about who will have access to their data once released. That is, they do not know if they can trust in a given service provider before interacting with it. In this document we have presented some challenges that current systems have to achieve.

User-centric techniques give more selection capabilities to the users in such a way that they can choose which digital identity they want to present to a specific service. Trust and reputation management systems are useful to identify malicious elements interacting in certain systems, especially in environments where strong trust agreements could not be supposed. Since these systems collects recommendations, based on past interactions, they are able to inform the users how a service will be, to some extent, before they interact with it.

We have described how user-centric techniques and trust and reputation systems could be integrated in identity management systems to achieve some of the presented challenges. Finally, we have analyze how these topics could be combined, in order to give more control and information to the users within identity management systems.

References

[1] Erdos, M., Cantor, S.: "Shibboleth-Architecture DRAFT v05", *I*nternet2/MACE 2002.

[2] Wason, T., Alliance, L., Hodges, J., Kemp, J., Thompson, P.: "Liberty Id-FF Architecture Overview", *L*iberty Alliance, 2003.

[3] Recordon, D. and Reed, D.: "OpenID 2.0: a platform for user-centric identity management", *P*roceedings of the second ACM workshop on Digital identity management (2006)

[4] Jones, M.B.: "The identity metasystem: A user-centric, inclusive web authentication solution", *T*oward a More Secure Web-W3C Workshop on Transparency and Usability of Web Authentication (2006)

[5] Higgins Personal Data Service: http://www.eclipse.org/higgins, (2007)

[6] Paquin, C. and Thompson, G.: "U-Prove CTP White Paper", *M*icrosoft Corporation (2010)

[7] Nanda, A. and Jones, M.B.: "Identity selector interoperability profile v1. 5", *M*icrosoft Corporation(2008)

[8] R. Aringhieri, E. Damiani, S.D.C. Di Vimercati, S. Paraboschi, P. Samarati: "Fuzzy techniques for trust and reputation management in anonymous peer-to-peer systems", *J*ournal of the American Society for Information Science and Technology vol. 57 n. 4, pp. 528537 (2006)

[9] M. Momani, S. Challa: "Survey of trust models in different network domains", *I*nternational Journal of Ad hoc, Sensor & Ubiquitous Computing vol. 1 n. 3, pp. 119 (2010)

[10] F. Gomez Marmol, M. Kuhnen, G. Martnez Perez : "Enhancing OpenID through a Reputation Framework", *P*roceedings of the 8th international conference on Autonomic and Trusted Computing ATC11, pp. 118 (2011)

[11] P. Guarda, N. Zannone : "Towards the development of privacy-aware systems", *I*nformation and Software Technology, vol. 51, n. 2, pp. 337350 (2009)