Risk Assessment for better Identity Management in Pervasive Environments

Patricia Arias Cabarcos (Phd Student)
Telematics Department, University Carlos III, Leganés, Madrid (Spain)

Abstract—**Pervasive computing environments comprise a myriad of devices. In this framework, interactions take place between different parties to simplify users' everyday life in a natural and transparent manner. These interactions, that are generally oriented to the delivery of services, usually involve the exchange of identity information and personal data over the networks. Since transactions may occur between familiar or unfamiliar entities, Identity Management (IdM) becomes indispensable to avoid security problems. Here, we aim to show that risk evaluation must be considered as a key enabler to foster collaboration between parties in a dynamic but yet secure manner. Taking this premise as a foundation, we are designing a methodology to assess risk. We also aim to integrate risk assessment with trust evaluation in order to aid in decision-making procedures, allowing the construction of flexible and dynamic IdM systems that are more suitable to be deployed in pervasive scenarios.**

I. Introduction

Pervasive computing environments, as envisaged by Weiser, comprise a myriad of devices: embedded sensors, actuators, computers, mobile terminals and the like. In these frameworks, interactions take place between different parties to simplify users' everyday life in a natural and transparent manner, even transcending human conscious. These interactions, that are generally oriented to the delivery of pervasive services (anytime, anywhere), usually involve the exchange of identity information and personal data over the networks.

In a ubiquitous world, whenever a change of context occurs (e.g. user enters a different location or new people in the proximity) new services and possibilities of interaction become available. It is important to note that in order for a user to gain access to pervasive services she should expose different forms of her identity. Furthermore, it is not realistic to assume that interactions always take place between known entities or that a previous trust relationship has been preconfigured by an administrator between every party in order to guarantee secure operations. Pervasive ambients are multiprovider and multiservice environments and so preconfiguration is not scalable. Thus, new mechanisms [1] must be introduced that mimic real life interactions, where people have to constantly decide who to trust or who to collaborate with in an open world.

In this sense, Identity Management (IdM) systems become indispensable to provide a seamless and secure user experience within the ecosystem of pervasive services. In fact, the concept of *federation* has gained special importance in recent years and many frameworks (SAML [2], OpenID [3], etc.) have been defined for this purpose. However, current federation technologies do not address the special requirements of open environments, so they suffer from limitations [4] that remain unsolved. Here, we aim to show that risk evaluation must be considered as a key enabler to foster collaboration between parties in a dynamic but yet secure manner. Taking this premise as a foundation, we introduce a novel way for risk quantification in federated IdM. We are also working on the integration of risk assessment with trust evaluation in order to aid in the decision-making procedures. This combination will allow the construction of flexible and dynamic IdM systems that are more suitable to be deployed in pervasive scenarios.

II. Enabling dynamic federations

The main goal of identity federation is to enable users of one domain to securely access systems of another domain seamlessly, and without the need for redundant user administration. The main actors in a federation scenario are: 1) the Identity Provider (IdP), which vouches for the identity of a user and issues authentication, authorization and/or attribute tokens; 2) the Service Provider (SP), which provides services to the end user and relies on the identity tokens generated by the IdP; and 3) the User, that interacts with SPs and IdPs.

In pervasive environments is especially remarkable the notion of personal federation (PN-F) [5] that refers to the establishment of relationships between Personal Networks belonging to different users (e.g. for cooperative services).

The problem of establishing federations in dynamic and open environments is that current technologies require trust and contractual frameworks to be preconfigured before any interaction between parties takes place. Thus, the initial setup complexity is a high barrier and may not worth adopting these procedures for a short-term collaboration because time and cost will probably not outbalance the rewards of cooperation.

Therefore, the main goals of our research are oriented to overcome the limitations of the current static features of IdM systems, and can be summarized in:

- Minimize dependence on preconfiguration, making entities autonomous and capable of taking trust decisions.
- Introduce a risk management model to enhance security.
- Take advantage of common knowledge.
- Enrich trust mechanisms (not only certificate-based trust).
- Allow seamless interaction.

As far as our work is concerned, in [4] we made a comparative analysis of the underlying trust models in IdM frameworks, which led us to assert that dynamic secure federation is not possible nowadays. Thus, we made a first proposal which consisted of adding new components and protocols so that

978-1-4244-9529-0/11/$26.00 ©2011 IEEE

entities could gather information and take dynamic decisions in real time by exploring the use of reputation data. Since then, an increasing interest has arisen around the possibility of adhoc dynamic federations [6]. In this document we describe our first approach to the risk management model.

III. Risk in Federated IdM

A. Importance and Challenges

Every actor that participates in a Federated IdM system has to take decisions that imply dealing with some form of risk. Thus, an IdP may ask itself if it is secure to collaborate with a particular unknown SP. Similarly, a SP will have to decide if it is secure to accept authentication statements issued by a specific IdP. And finally, it is crucial that the user is aware of the transactions regarding her identity. In fact, she should be provided with some kind of risk information to determine if she should reveal her personal data to a SP or IdP.

It is worth mentioning that most of the related work on the topic simply states that risk should be considered in decision making processes. However, works defining how to assess risk are scarce. Furthermore, the nature of these proposals is mainly qualitative and there is a lack of completeness, since the user interests are ignored. These limitations led us to propose a methodology to assist in risk quantification.

B. A metric-based approach to assess risk

The first step for risk quantification is to collect data and extract significant numerical values, the metrics, that could be used later, together with statistics and probability theory, to conform a risk model.

We argue that Federated IdM consists of two different phases that should be analyzed separately to evaluate risks:

- **Pre-Federation Phase**, wich encompasses the establishment of a relationship and the exchange of all the required information to engage in cooperation. It can be understood as a **Bootstraping Phase**.
- **Post-Federation Phase**, which contemplates the transactions between two federated entities . This stage can be viewed as the **Evolution Phase**, since entities progressively construct and consolidate their relationships.

The decisions to take, the actors participating and the available information are different in each phase; and so are the faced risks. Based on the above distinction, we have designed a risk taxonomy[1], which should be adopted by every entity in the IdM system to enrich its intelligence and independence and to be capable of taking well-informed decisions. The proposed risk taxonomy contemplates a first level under the Pre-federation and Post-federation phases in order to capture Security, Interoperability, Trust and Service-Specific risks. Then, another subdivision is made to cover risks associated to the basic security services (Confidentiality, Integrity, Authentication and Non-repudiation), as well as risks related to the direct and indirect facets of trust. The final level in the taxonomy reflects the categories of transport and application risks. In conclusion, the classification compiles the characteristics of Federated IdM systems and makes possible risk decomposition in small subsets. So, it is used as a central piece to the risk identification procedure in order to derive appropriate metrics to use in quantification.

Thus, we are currently working on this novel methodology to identify risk metrics that will be used to implement a risk calculation module and complete a prototype entity capable of engaging in more secure dynamic federations. So, the ideas in this paper should be understood as a subset of a broader study aimed at defining a generic infrastructure that favours cooperation between parties in a flexible and dynamic manner.

In order to evaluate our proposals, an IdM infrastructure has been deployed that consists of IdPs, SPs and active clients. Then, we have introduced some of the modifications proposed in [4]: SAML extension to ask for reputation data and development of a *proof-of-concept* application to show the viability of the proposal. Currently, we are working on the collection of metrics to make risk quantification possible.

IV. Conclusions and Future Work

Our research focus on the establishment of dynamic adhoc federations, which are indispensable to allow seamless secure interactions in the emerging multiservice ubiquitous reality. So far, we have: 1) analyzed the limitations of current IdM frameworks; 2) proposed and partially implemented an extension to SAML that allows to take dynamic decisions in federated IdM based on reputation. Now, we are working on risk evaluation to enrich the decision procedures. The main steps in this regard are identification of a comprehensive set of metrics, calculation and aggregation of values, as well as testing for usefulness and efficiency of the model.

More generally, we identify the following tasks as future working lines: model the relation between risk and trust evolution, study how to define contexts for reputation and other trust dimensions, add support for delegation use-cases, and perform evaluation tests in more complex scenarios.

Acknowledgment

This work has been partially funded by University Carlos III of Madrid in the context of project D.I.MAN.D.S 2010/00191/001. The author wants to thank Florina Almenárez (supervisor) and Andrés Marín for their guidance and valuable comments to this PhD proposal.

References

[1] F. Almenárez et al., *Developing a model for trust management in pervasive devices.* PerCom Workshops 2006. New york, 2006. 271276.

[2] S. Cantor et al., *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, 2005.

[3] OpenID. *OpenID Authentication 2.0.* December 2007.

[4] P. Arias et al., *Enabling SAML for Dynamic Identity Federation Management.* Wireless and Mobile Networking Conference (WMNC'09).

[5] J. Hoebeke et al., *Personal networks federations*, presented at 15th IST Mobile and Wireless Summit, Myconos, Greece, June 2006.

[6] Draft ETSI GS INS-004 V 0.0.5 (2010-01), Group Specification. *Identity and access management for Networks and Services; Dynamic federation negotiation and trust management in IdM systems.*

[1] the schematic of the risk taxonomy is not included in the present document due to the lack of space