Web of Trust Enhanced Authentication Levels of Assurance (WoT4LoA)

Bob Hulsebosch[1], Maarten Wegdam[1], Martijn Oostdijk[1], Jaap Reitsma[1], Joost van Dijk[2], Pieter van der Meulen[2] & Remco Poortinga – van Wijnen[2]

[1] Novay, PO Box 589, 7500 AN, Enschede, the Netherlands
[2] SURFnet, PO Box 19035, 3501 DA, Utrecht, the Netherlands

e-mail: Bob.Hulsebosch@novay.nl, Martijn.Oostdijk@novay.nl, Maarten.Wegdam@novay.nl, Jaap.Reitsma@novay.nl, Joost.vanDijk@surfnet.nl, Pieter.vanderMeulen@surfnet.nl, Remco.Poortinga@surfnet.nl

Keywords: strong authentication, LoA, web of trust

Introduction

In higher research and education and its identity federations there is an increasing need for stronger authentication solutions that go beyond username and password.

The strength of the authentication solution is usually expressed in terms of levels of assurance (LoA). Two factors are essential in determining the LoA:

1. The strength of the processes used for identity proofing, registration, and the delivery of credentials that bind an identity to a token.
2. The strength of the authentication mechanism to establish that a user is who he claims to be, which in turn mainly depends upon the strength of the authentication solution (passwords, token, smart card, etc.).

Though many authentication solutions are available, not all of them are suitable for application in higher education and research and their identity federations. Aspects like costs, enrolment effort and user friendliness need to be taken into account.

Particularly, the process by which to link a physical person to his/her digital identity information and to his/her authentication credentials during enrolment is critical to deter registration fraud. If this is done poorly, there is little or no assurance that the person using that credential is who he/she claims to be. A solid registration process, however, is expensive as it usually requires the establishment of a registration desk and is not very user friendly, as he/she has to go to the registration desk. The latter requirement can even be impossible to meet for remote users.

Web of trust enhanced authentication

WoT4LoA is a Géant3plus Open Calls project that tries to address the issue of strong authentication in higher education and research. The ambition of WoT4LoA is to achieve stronger authentication without the cost and overhead of physical registration and complexity of many other remote registration solutions. The idea is to use the web of trust concept to establish the authenticity of the

binding between an authentication solution (e.g. public key) and its owner via third party user attests. For instance, if person A claims that user B is using a particular authentication solution, it can provide extra confidence for the service provider to allow access to resources that require stronger authentication. Person C can also claim to know B and his authentication mechanism, thereby even further increasing the trust in the identity of B. This approach is a kind of "crowdsourcing of trust" about the identity of the user. A concrete example is the use of the mobile phone as a second authentication factor. Other users can make attests towards the identity provider about the number of the mobile phone of a particular user allowing it to be used as a reliable second factor during e.g. a step-up authentication scenario.

The concept of web of trust based LoA enhancement in a federation setting is illustrated in Figure 1. In a federation the identity provider (IdP) typically authenticates the user when he makes an access request at a service provider (SP). In the web of trust based LoA approach, other users (Eve and Alice) in the federation attest towards the IdP that they know the user (Bob). This increases Bob's LoA.

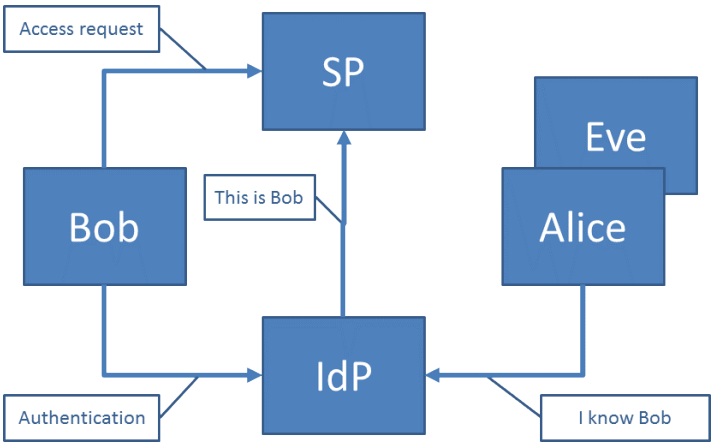

Figure 1: Web of trust based LoA enhancement in a federation setting.

The attests of other users easily fit into the "claims" architecture of the federated identity infrastructures. Moreover, the social or research context of the user can be effectively used to enhance the registration part of an authentication solution. Particularly in the context of research groups or virtual organizations in which users know each other, a web of trust based authentication enhancements can effectively be executed. This approach also makes it easier to use social identities provided by e.g. Facebook and Google in higher education and research environments. The strength of the authentication provided by these popular social identity providers is relatively weak. Web of trust based enhanced authentication helps to improve it.

Challenges

The web of trust approach also has its weaknesses. Possible threats amongst others are whitewashing and Sybil attacks, impersonation and reputation theft, bootstrapping issues, extortion, denial-of-reputation, ballot stuffing and bad mouthing, recommender dishonesty, privacy threats for voters and reputation owners, social threats such as discrimination or risk of herd behaviour, attacking of the underlying infrastructure and the exploitation of features of metrics used by the system to calculate the identity assurance. These threats need to be taken into account to evaluate

usefulness of the web of trust-based solution to enhance the LoA in the context of identity federations.

A potential improvement to traditional web of trust systems revolves around reducing the validity period of the claims made by other users regarding a specific user account and to allow for automatic prolongation of the trust-based claims associated to the account by subsequent authentication sessions. This allows for both verification of use of the account and the identity associated to it and user revocation of 'stale' or otherwise undesired credentials. During the refresh process, the user can choose whether to continue or stop endorsing others' accounts; this helps the dynamics of the web by helping to cull out untrusted persons more rapidly.

Further, providing the option for anti-claims, to specifically call out an account as untrusted to others, significantly mitigates the effect of malicious persons such as spammers gaining access to a web of trust. Allowing for this anti-measure also forms the basis of a sliding trust scale, with trust and anti-trust counting against each other and allowing for identity providers to see that a particular account may or may not be trustworthy.

A web of trust based LoA approach raises several other challenging research questions that need to be addressed, such as: what are possible use cases, approaches and protocols to implement the web of trust model to increase the authentication strength, how to define the metric to determine a certain authentication level and what factors need to be taken into account in this metric (number of claims, quality of the claims, history of the claims, …), how to guarantee the authenticity of the claims made by others, how to leverage the web of trust enhanced authentication within a virtual organization or research group context where users typically know each other, and what is the impact of this approach on the identity providers that are responsible for user authentication?

At TNC2014 the first answers to these challenges will be presented.

Acknowledgements

This work is sponsored by Géant3plus Open Calls program.

Vitae

Bob Hulsebosch, Martijn Oostdijk and Maarten Wegdam are senior researchers at Novay. Both have more than 10 years experience in ICT research, consultancy and project management in the areas of federated identity, authentication, privacy and trust. Jaap Reitsma is a senior research engineer experienced in implementing federated identity solutions.

Pieter van der Meulen, Joost van Dijk and Remco Poortinga-van Wijnen are members of the Middleware Services department of SURFnet and are involved with various technical and operational identity and trust aspects in the SURFconext federation.