Security 2.0: Trusted Identity Service

Vanessa Alvarez[1], Antonio Amaya[1], Miguel Ochoa[1], David Prieto[1]

[1] Telefonica I+D
{vac, amac, ochoa, dprieto}@tid.es

Abstract. Social network interactions need a recompilation of information that can be used to evaluate the trust that can be deposited on each peer. Existing solutions centered on service providers have both quantitative and qualitative limitations. We introduce a new approach based on a Trusted Identity Service located on the access provider that will provide service providers with information about a global and unchangeable trust level of the users.

1 Introduction

Internet services boom imply an increase of private and confidential information deposited by individuals and companies on the service providers. There's also a constant increase of the economic value of the online transactions.

At the same time the economic value and type distribution of cybercrime is increasing. New cybercrime types include identity theft and stealing of personal data to be used on Internet frauds –like stealing of money from bank accounts and buying with stolen credit cards, or distributing unwanted mail or publicity to the contact list of the compromised person- or real world crime –get personal information from person to blackmail them, steal on his home..- Because of all this it's necessary having mechanisms that allow the users to evaluate the trust level they can deposit on a peer on any online transaction.

While security and trust on the real world is based and relies usually on physical presence of the peers involved on any transaction on the same location – that way documents, physical aspect or signatures may be verified in situ, and thus the trust level of the peers may be established- on Internet there's no such possibility, since peers communicate remotely from locations on any part of the world, and they interact using computing devices and communication media that can be controlled by third parties.

Thus, during electronic transactions there's a recompilation of information that can be used to evaluate the trust that can be deposited on each peer, protecting the information that's being used, avoiding an illicit use of the information, on that same or a later moment.

On one hand, users accessing a service provider have different methods to evaluate the trust level of the service provider using server certificates, web filtering services, …

On the other hand, service providers also need to evaluate during electronic transactions the trust level they can deposit on any user – is he the one he says he is?

Is he using a secure device and communication channel, on which the confidential information is secure against a later illicit use? To this extent, there are also several solutions that get useful information to evaluate the trust level using user identification mechanisms based on several authentication factors, solutions like firewalls and antimalware that try to avoid information theft on the customer's device, solutions that provide a service provider some other information that can be used to evaluate the trust level like usual or close to a recent usual IP address, browser known security exploits, …

Depending on the risk assessment, a service provider can make several decisions: it can reject the user or ask him for a different level of authentication. Our solution is centered on the evaluation, by the service provider, of the trust that he can assign to the user, behaving in that way like a "trust authority".

1.1 Problems with existing solutions

Social network sites have to evaluate the trust level of the user trying to access its services and this trust evaluation depends on the quantity and quality of available data.

As a part of that trust determination process, a service provider has to answer the questions: is the user the one he says he is? Is he accessing our servers from a secure environment (location, device) on which confidentiality and security of transmitted data will be assured? To that extent they use information they have available, related with electronic communications like security of the equipment/device the user is using to access the service, user location, user's behavioral analysis or user's authentication.

But usage of electronic communications information by part of the service providers with current techniques has a quantitative limitation due to the problem of using partial information, and a qualitative limitation because this information can be manipulated by malicious attackers. Current systems also require that the user uses specific mechanisms for each service provider (authentication mechanisms, antimalware software). This might hinder user's enjoyment of the services if he usually accesses several service providers.

2 Trusted Identity Service

The solution proposed is based on a trust generation system located on the access provider that will provide service providers with information about the trust level of the users. This information will be more complete and of more quality than the information the service providers are using actually. This way the access provider will become a 'trust authority'.

This is accomplished by gathering information directly on the Internet access provider that the users are using to contact service providers. A device located on the access provider internal network gathers information about: user's identity, user's traffic that will be used to analyze his behavior, security status of the user's device, and geographical location. All this information is analyzed and summarized on a ‘trust ticket’ that will be sent to service providers.

The defined system will provide service providers with the trust level they can assign to a given user more complete and with more quality than the one they’re currently using, since the trust level will be based on information gathered directly on the network access provider that the user’s are using to connect to the service providers. This information is more difficult to manipulate by malicious third parties than the information service providers are currently using; thus, IP address used as part of the analysis is assigned by the network access provider and cannot be manipulated as it could be if the service provider were getting the IP from the user’s device.

2.1 Security as a Service Capability

Telcos have chosen a Service Oriented Architecture (SOA) as a base of their Service Delivery Platform (SDP) for applications, services and contents distribution. SDP allows to Telco’s enterprises to increase incomes per user with new added-value services, reducing development, deployment and operational costs. SOA technology provides the integration of different systems on a consistent environment where the existing assets can be re-use to create a new value, where time to market is reduced from months and years to days and weeks.

So security functionalities that are deployed as network capacities can be used alone or in an aggregate form (multifactor security) by third-party applications, Telco’s applications or by other elements within the SDP architecture, to enrich their functionalities, increase user loyalty or increase the security level which is developed.

2.2 Privacy by Design

The Trusted Identity Service developed as a RESTful web service, even though shown in an aggregate form, discloses user personal information. So, we use OAuth protocol for intercepting queries that come from online services that act as consumers, conducted to this resource and checking that they hold a valid authorization ticket issued by the personal information owner.

Moreover, OAuth [1] extension has been developed to introduce a privacy policy associated to the lifetime and uses of authorization tickets.

3 Conclusion

Global social network services require global and trusted identity services. Access providers have a global and unchangeable knowledge of users and services to become a ‘trust authority’. This Trusted Identity Service can be exposed as a SDP Service Capacity to service providers but from the beginning conforming to privacy principles of visibility, transparency and respects for user privacy.

Acknowledgments. This work has been developed by Telefonica I+D and funded by the Centre for the Development of Industrial Technology (CDTI) of Spain, within the framework of the Segur@ project [2], reference CENIT-2007 2004 of the CENIT Program (part of the INGENIO 2010 initiative).

References

1. OAuth, http://oauth.net
2. Proyecto SEGUR@ - Seguridad y Confianza en la Sociedad de la Información”, http://www.cenitsegura.com