Chapter 24

Trusted Computing or Distributed Trust Management?

Michele Tomaiuolo
Università di Parma, Italy

ABSTRACT

Nowadays, in contrast with centralized or hierarchical certification authorities and directory of names, other solutions are gaining momentum. Federation of already deployed security systems is considered the key to build global security infrastructures. In this field, trust management systems can play an important role, being based on a totally distributed architecture. The idea of distributed trust management can be confronted with the concept of trusted computing. Though having a confusingly similar denomination, the different interpretation of trust in these systems drives to divergent consequences with respect to system architectures and access policies, but also to law, ethics, politics. While trusted computing systems assure copyright holders and media producers that the hosting system will respect the access restrictions they defined, trust management systems, instead, allow users to grant trust to other users or software agents for accessing local resources.

INTRODUCTION

A number of architectures and systems are being proposed as a ground for improved interoperability among diverse systems, mainly exploiting the idea of service-oriented architecture. Yet, some issues remain open. In fact, composition of services requires some delegation of goals and duties among partners. But these delegations cannot come into effect, if they’re not associated with a corresponding delegation of privileges, needed to access some resources and complete delegated tasks, or achieve desired goals.

The traditional approach for inter-domain security is based on centralized or hierarchical certification authorities and public directory of names. In contrast with this hierarchical approach, other solutions are possible, where the owner of local resources is considered as the ultimate source of trust about them, and he is provided...
with means to carefully administer the flow of delegated permissions. *Trust management* principles argue no a-priori trusted parties should be supposed to exist in the system, as this would imply some “obligated choice” of trust for the user, and without *choice*, there’s no real *trust*. Moreover, the presence of some third party as a globally trusted entity implies that all systems participating in the global environment have to equally trust it.

Nowadays, new technologies, in the form of protocols and certificate representations, are gaining momentum. They allow a different approach toward security in global environments, an approach which paradoxically is founded on the concept of “locality”. Federation of already deployed security systems is considered the key to build global security infrastructures. This way, users are not obliged to adopt some out of the box solution for their particular security issues, to rebuild the whole system or to make it dependent upon some global authority, for gaining interoperability with others.

Instead they’re provided with means to manage the trust relations they build with other entities operating in the same, global environment. In the same manner as people collaborate in the real world, systems are being made interoperable in the virtual world. Cooperation and agreements among companies and institutions are making virtual organizations both a reality and a necessity. But they’ll never spring into success if existing technologies will not match their needs.

This chapter will deal with trust management in open and decentralized environments. Up-to-date technologies like SAML, OpenID, XRI, XDI, XACML, Web Services protocols and extensions, will be analysed from the perspective of *peer to peer* networks, intended not only as a technology, but above all as a web of trust relationships, where parties interoperate directly, without reliance on any centralized directory or authority.

Securing access to the resources made available by the peers is a requirement to make peer to peer interoperation a more widespread paradigm. The secure management of trust relationships, the ability to precisely control the flow of delegated permissions to trusted entities, is a fundamental requirement to allow the composition of the more disparate services provided on the network.

This chapter will also analyse the fundamental differences between decentralized trust management, on the one hand, and digital rights management and trusted computing, on the other hand. The different interpretation of *trust* in these systems drives to divergent consequences with respect to system architectures and access policies, but also to law, ethics, politics. While *trusted systems* assure *copyright holders* and *media producers* that the hosting system will respect the access restrictions they defined, *trust management systems*, instead, allow *users* to grant trust to other users or software agents for accessing local resources.

The analysis will start from XrML and ODRL, two similar XML-based languages oriented to the management of digital rights for media content distribution. Both languages are oriented to the management of digital rights (DRM) for publishing and accessing media content, and can hardly fit different applications. In fact, these Rights Expression Languages resulted from efforts of businesses to protect digital material from reproduction and sharing. They just allow copyright owners to express restrictions about the usage of a resource, without being able to enforce by themselves the policies they convey. This can only happen on so-called “trusted systems”. Support for DRM is being included into a growing number of devices and systems. The international legal framework is also paying attention to DRM systems. Many nations adhering to the World Intellectual Property Organization (WIPO) are implementing the 1996 WIPO Copyright Treaty (WCT), which requires to enact laws against DRM circumvention. The 1998 Digital Millennium Copyright Act (DMCA) in the USA and the 2001 European directive on copyright (EUCD) are two important examples.