A Critical Comparison of Trusted Computing and Trust Management Technologies

Michele Tomaiuolo, Department of Information Engineering, University of Parma, Parma, Italy

ABSTRACT

Mainly justified by the growing concern about vulnerabilities of IT systems, some new technologies are being integrated into computing devices, for realizing so-called Trusted Computing systems. However, they are raising questions about intrusive cyber-control over individual user activities and data, but also about consequences in cyber-war scenarios. The aim of this article is to confront Trusted Computing systems with distributed Trust Management systems, which realize access control for local resources on the basis of delegation of access rights, according to local trust decisions. Both technologies are discussed from various points of view: architecture, vision, ethics, politics and law. Some experimentations are also presented, to show the applicability of Trust Management techniques to modern Service-Oriented Architectures.

Keywords: *Authorization, Delegation, Digital Books, Information Access, Intellectual Property Rights, Multimedia, Security, Trust, Web Services*

INTRODUCTION

The growth of attacks to computing systems, as well as the privacy issues emerging in many popular communication technologies, are attracting more attention to the overall security of ICT systems and infrastructures (Franchi, Poggi and Tomaiuolo, 2014). A central issue is the protection of resources from unauthorized access, which relates to the additional issues of secure user authentication, definition and enforcement of access policy, reliable accounting, confidentiality and integrity of data.

A new wave of technologies and standards, in particular, deals with the enforcement of a "trusted environment" on a wide range of devices, from embedded and pervasive systems to servers. Such technologies are often referred to as Trusted Computing (TC) and have the declared objective of executing applications and storing data in a secure way. Intel, for example, cites the rising tide of malware and other attacks through malicious programs as one of the main motivation for its new Trusted Execution Technology (Greene, 2012). However, the environment set up by Trusted Computing

DOI: 10.4018/ijcwt.2014100105

technologies is also fit for implementing Digital Rights Management (DRM) systems. In fact, a "trusted system" can attest to copyright holders that access policies for protected media files will be earnestly enforced. Moreover, especially taking into account the potential collaboration of technology vendors with nation states (Jøsang, 2014), these systems may pave the way to new form of cyber-warfare.

Another approach to access control is based on decentralized Trust Management (TM), i.e. on the peer-to-peer delegation of access rights among users. In Trust Management systems, in fact, the administrator of local resources is considered as the ultimate source of trust about them, and is provided with means to carefully regulate the flow of delegated permissions. No a-priori trusted parties are supposed to exist in the system, in general. This can also represent the basic setting for improved interoperability among diverse systems.

This article presents both TC and TM architectures, which in some sense are orthogonal and also complementary. However, their visions are at contrast, with regards to overall centralized or hierarchical control and user empowerment. The following section provides an overview of DRM technologies, Trusted Computing architectures and the supporting legal framework for dealing with infringements. Then, the principles of Trust Management for peer-to-peer delegation and some strategies and issues of Trust Negotiation are described. Also, the dDelega library is introduced, as an original example of use of the distributed delegation and negotiation mechanisms of TM in the context of Web services. Finally, a critical comparison between the different approaches to trust building and enforcing is provided, together with other concluding notes.

TRUSTED SYSTEMS

Regarding the basic architecture and functioning of Digital Rights Management systems, various so-called "Rights Expression Languages" have been proposed, for the management of digital rights for media content distribution. These languages and frameworks are essentially the result of efforts of businesses to protect digital material from reproduction and sharing. However all Rights Expression Languages just allow copyright holders to express restrictions about the usage of a resource (for this reason, critics of those technologies often refer to them as "restrictions expression languages"), without being able to enforce by themselves the policies they convey. The usage of "trustworthy" systems (Coyle, 2003) and the application of international laws is necessary for actually enforcing the policies these languages allow to express.

Obfuscation is necessary for the realization of DRM restrictions on common PCs and other open systems, to make reverse engineering more difficult and protect in some way the decryption function. But in traditional cryptography, obfuscation has always been considered a poor solution, with uncertain resistance to attacks. In fact, obfuscation is the Achille's heel of most DRM systems (Stamp, 2003). Moreover, in open systems the decryption function (generally a cryptographic key) can be gathered by scanning the system memory at runtime.

To overcome this problem, content producers are encouraging laws against circumvention of DRM policies. But another parallel effort is directed toward the realization of so-called Trusted Computing systems, composed only of approved hardware and software components, which can assure the respect of media access restrictions.

Digital Rights Management

DRM infrastructure is being included into a growing number of devices and systems, with the support of ICT firms, together with content producers and distributors. In computer systems and other devices, DRM technologies can be found at different levels: (*i*) hardware, e.g., the Content Scramble System (CSS) of DVD players; (*ii*) operating system, e.g. the Rights Management System (RMS) of Microsoft Windows Server 2003; and (*iii*) application, e.g.

Security Risks to IT Supply Chains under Economic Stress

C. Warren Axelrod and Sukumar Haldar (2013). *International Journal of Cyber Warfare and Terrorism (pp. 58-73).*
www.igi-global.com/article/security-risks-to-it-supply-chains-under-economic-stress/105193?camid=4v1a